대한민국 특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2002-0086889
Application Number

출 원 년 월 일 : 2002년 12월 30일
Date of Application DEC 30, 2002

출 원 인 : 박승배 외 1명
Applicant(s) PARK, SEUNG BAE, et al.

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

2003 년 09 월 08 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2002.12.30
【발명의 명칭】	패스워드 입력을 위한 사용자 인터페이스와 패스워드 입력 방법 그리고 이를 이용한 패스워드 시스템
【발명의 영문명칭】	USER INTERFACE AND METHOD FOR INPUTTING PASSWORD AND PASSWORD SYSTEM USING THE SAME
【출원인】	
【성명】	박승배
【출원인코드】	4-1999-026827-9
【지분】	90/100
【출원인】	
【명칭】	주식회사 크립존
【출원인코드】	1-2002-029695-1
【지분】	10/100
【대리인】	
【성명】	김용대
【대리인코드】	9-1999-000402-4
【포괄위임등록번호】	2002-092049-4
【포괄위임등록번호】	2002-092048-7
【발명자】	
【성명】	박승배
【출원인코드】	4-1999-026827-9
【우선권주장】	
【출원국명】	KR
【출원종류】	특허
【출원번호】	10-2002-0047012
【출원일자】	2002.08.09
【증명서류】	미첨부
【심사청구】	청구

10[redacted]086889 출력 일자: 2003/9/18

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
김용대 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	52	면	52,000 원
【우선권주장료】	1	건	26,000 원
【심사청구료】	37	항	1,293,000 원
【합계】	1,400,000 원		
【감면사유】	소기업 (70%감면)		
【감면후 수수료】	438,200 원		

【첨부서류】 1. 요약서·명세서(도면)_1통 2.지분약정서_1통 3.소기업임을 증명하는 서류_1통

【요약서】

【요약】

여기에 패스워드 시스템이 제시되고, 제시된 패스워드 시스템에서 사용자를 인증하는 방법이 기술된다. 본 발명의 패스워드 시스템은 패스워드 입력 과정을 관찰한 타인에게 패스워드가 노출되는 것을 방지할 수 있는 새로운 패스워드 입력 방법과 이에 적합한 사용자 인터페이스를 제공하는 진보된 패스워드 시스템이다. 사용자 인터페이스는 적어도 두 개의 기호 보드를 제공하고, 사용자에게 제공되는 매칭 수단을 통해 두 개의 기호보드에 나열된 기호들이 매칭되어진다. 이때, 패스워드 입력을 위해 매칭되는 기호들과 이를 위장하기 위한 다수의 기호들이 동시에 매칭됨으로서 관찰자는 어느 기호의 매칭이 패스워드 입력을 위한 매칭인지를 구분할 수 없다.

【대표도】

도 10

【명세서】

【발명의 명칭】

패스워드 입력을 위한 사용자 인터페이스와 패스워드 입력 방법 그리고 이를 이용한 패스워드 시스템{USER INTERFACE AND METHOD FOR INPUTTING PASSWORD AND PASSWORD SYSTEM USING THE SAME}

【도면의 간단한 설명】

도 1a 및 도 1b는 본 발명의 패스워드 입력 방법을 설명하기 위한 도면으로 도 1a는 매칭 전의 숫자열을 도 1b는 매칭 후의 숫자열을 각각 보여주는 도면;

도 2는 본 발명의 패스워드 입력 방법을 집합 개념으로 일반화하여 설명하기 위한 개념도;

도 3a는 도 1a에 도시된 숫자열에서 사용된 실상매칭기호와 허상매칭기호 그리고 실상패스워드기호와 허상패스워드기호를 각각 지적하여 표시한 도면;

도 3b는 도 1b에 도시된 매칭된 숫자열에서 매칭된 RMS와 RPS, 매칭된 VMS와 VPS 그리고 매칭된 기호 모임을 각각 지적하여 표시한 도면;

도 4a 내지 도 4d는 다수의 기호 매칭 과정을 반복 수행하여 투-패스워드를 입력하는 예를 설명하기 위한 도면;

도 5a 내지 도 5d 그리고 도 6a 및 도 6b는 투-패스워드로부터 RMSG와 RPSG를 생성하는 다양한 예를 보여주는 도면;

도 7은 본 발명의 투-패스워드 시스템과 이를 채용한 메인 시스템과의 관계를 보여주는 블록도;

도 8은 본 발명의 투-패스워드 시스템과 사용자 인터페이스의 구성을 보여주는 도면;

도 9는 본 발명의 투-패스워드 시스템의 인증 프로세스를 개략적으로 보여주는 플로우차트;

도 10은 메인 시스템에 따른 사용자 인터페이스의 일 실시예를 보여주는 도면;

도 11a 내지 도 11d는 기호보드의 다양한 변형예를 보여주는 도면;

도 12는 제1 기호보드가 생략되어 표시되는 변형예를 보여주는 도면;

도 13은 제1 기호보드와 제2 기호보드의 표시 형태를 교환 표시한 다른 변형예를 보여주는 도면;

도 14는 제2 기호보드에 다수개의 기호열을 동시에 표시하는 또 다른 변형예를 보여주는 도면;

도 15는 기호매칭을 위해 기호보드의 순환 이동량을 입력하기 위한 입력창을 제공하는 그래픽 사용자 인터페이스의 일 예를 보여주는 도면;

도 16은 기호열을 순환 매칭시키기 위한 다수의 입력 버튼을 구비한 그래픽 사용자 인터페이스의 일 예를 보여주는 도면;

도 17은 기호보드가 자동 순환하는 경우의 그래픽 사용자 인터페이스의 일 예를 보여주는 도면;

도 18은 본 발명의 투-패스워드 시스템을 탑재한 도어락 시스템을 위한 사용자 인터페이스의 일 예를 보여주는 도면;

도 18은 전자 회로와 연동한 투-패스워드 시스템의 사용자 인터페이스의 일 예를 보여주는 도면;

도 19는 하나의 기호보드만을 표시하는 변형예를 보여주는 도면;

도 20은 도 18의 사용자 인터페이스의 회로 구성의 일 예를 보여주는 도면;

도 21은 기계적 메커니즘과 연동한 투-패스워드 시스템의 사용자 인터페이스의 일 예를 보여주는 도면;

도 22는 도 21의 사용자 인터페이스의 회로 구성의 일 예를 보여주는 도면;

도 23에 패스워드기호보드의 회전수를 소정의 범위 이내로 하기 위한 기호 나열의 일 예를 보여주는 도면;

도 24a 내지 도 24d는 매칭된기호모임의 일 예를 설명하기 위한 도면;

도 25는 도 24a 내지 도 24d에서 매칭된기호모임을 표로 보여주는 도면;

도 26은 패스워드 인증처리의 구체적인 프로세스를 보여주는 플로우차트;

도 27은 투-패스워드로부터 유도된 RMSG와 매칭되는 MSG의 기호들을 보여주는 도면;

도 28 및 도 29는 메모리에 저장된 인증기준정보의 일 예를 보여주는 도면;

도 30은 본 발명의 투-패스워드 시스템이 스탠드얼론 시스템에 탑재되는 경우의 일 예를 보여주는 도면;

도 31은 본 발명의 투-패스워드 시스템이 네트워크 환경에서 메인 시스템에 탑재되는 경우의 일 예를 보여주는 도면; 및

도 32는 네트워크 환경에서 투-패스워드 시스템이 통신 단말기에 탑재되는 경우의 일 예를 보여주는 도면이다.

* 도면의 주요 부분에 대한 부호의 설명 *

10: 사용자 20: 사용자 인터페이스

30: 투-패스워드 시스템 40: 메인 시스템

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<36> 본 발명은 패스워드 시스템(password system)과 이의 사용자 인터페이스(user interface)에 관한 것으로, 구체적으로는 패스워드 입력 과정을 관찰한 타인에게 패스워드가 노출되는 것을 방지할 수 있는 새로운 패스워드 입력 방법과 이에 적합한 사용자 인터페이스를 제공하는 진보된 패스워드 시스템에 관한 것이다.

<37> 사용자 인증 시스템은 여러 장치나 시스템에 널리 사용되고 있다. 사용자 인증은 시스템 접근자가 인가된 사용자인가를 확인하는 것이다. 실환경에서 사용자 인증은 사용자 인증 시스템에 의하여 구체화된다. 사용자 인증 시스템은 소프트웨어나 소프트웨어와 하드웨어가 결합된 것으로, 사용자가 제공하는 정보와 시스템에 저장되어 있는 정보를 이용하여 사용자 인증을 한다.

<38> 사용자가 제공하는 정보로는 기억하고 있는 정보나 소유하고 있는 매체에 저장되어 있는 정보, 생체 정보가 있다. 기억하고 있는 정보의 예로는 id와 패스워드가 있으며, 소유하고 있는 매체의 예로는 카드가 있고, 생체 정보의 예로는 지문이 있다.

39> 일반적으로 사용자가 기억하고 있는 정보를 이용하는 사용자 인증 시스템은 소프트웨어이고, 매체나 생체 정보를 이용하는 사용자 인증 시스템은 소프트웨어와 하드웨어가 결합된 것이다. 소프트웨어와 하드웨어가 결합된 사용자 인증 시스템의 예로서, 지문 인식 시스템은 지문 정보를 입력 받기 위한 지문 인식 장치와 디지털 지문을 처리하는 소프트웨어로 구성되어 있다.

40> 패스워드 시스템은 사용자가 기억하고 있는 정보를 이용하는 사용자 인증 시스템으로, 사용자가 ID와 패스워드를 입력하는 방식의 패스워드 시스템이 가장 보편적으로 사용되고 있다. 패스워드 시스템은 시스템 관련 모듈과 사용자 인터페이스 관련 모듈을 포함하고 있다. 그리고, 암호 기술을 구현한 모듈은 시스템에 따라 선택적으로 사용된다.

41> 일반적으로 사용자 수가 일인인 시스템의 패스워드 시스템은 암호 모듈이나 다른 보안 플랫폼 모듈을 포함하고 있지 않으며, 이러한 시스템의 예들로는 데스크 탑 얼론과 셀룰러 폰이 있다. 일반적으로 사용자 수가 다수인 시스템의 패스워드 시스템은 암호 모듈이나 다른 보안 플랫폼 모듈을 포함하고 있으며, 이러한 시스템의 예들로는 공개 키 기반구조를 이용하는 인터넷 뱅킹 시스템과 UNIX 시스템이 있다.

42> 패스워드 시스템은 사용이 편리하고 가격이 저렴하며, 구현이 쉽다는 등의 장점으로 인하여 가장 보편적으로 사용되는 사용자 인증 시스템이지만, 기존 패스워드 시스템은 사용자가 패스워드를 입력하는 과정을 관찰한 타인에게 패스워드가 쉽게 노출된다는 단점이 있다.

【발명이 이루고자 하는 기술적 과제】

<43> 따라서 본 발명의 목적은 사용자의 패스워드 입력 과정이 타인에게 노출되어도 관찰자가 입력된 패스워드를 알 수 없도록 하는 패스워드 입력 방법을 제공하는데 있다.

<44> 본 발명의 다른 목적은 패스워드 입력 과정을 관찰한 타인이 입력된 패스워드를 감지할 수 없게 하는 패스워드 입력을 위한 사용자 인터페이스를 제공하는데 있다.

<45> 본 발명의 또 다른 목적은 패스워드 입력 과정을 관찰한 타인이 입력된 패스워드를 감지할 수 없게 하는 패스워드 입력 방법에 적합한 인증프로세스를 구비한 패스워드 시스템을 제공하는데 있다.

【발명의 구성 및 작용】

<46> 상술한 바와 같은 본 발명의 목적을 달성하기 위한 본 발명의 일 특징에 의하면, 패스워드 시스템은: 매칭에 기준이 되는 하나의 실상매칭기호와 실상매칭기호를 위장하기 위한 다수의 허상매칭기호를 포함하는 다수의 기호들이 나열 표시되는 매칭기호보드, 실상매칭기호와 매칭되어야 하는 하나의 실상패스워드기호와 실상패스워드기호를 위장하기 위한 다수의 허상패스워드기호를 포함하는 다수의 기호들이 나열 표시되는 패스워드기호보드를 표시하는 표시수단; 매칭기호보드와 패스워드기호보드에 표시될 기호모임을 생성하는 기호발생수단; 기호발생수단에서 생성된 기호모임에 대한 정보를 받아들여 매칭기호보드와 패스워드기호보드에 나열 표시하는 표시제어수단; 사용자가 실상매칭기호와 실상패스워드기호를 매칭시키기 위한 매칭수단; 매칭수단에 의해 매칭기호보드와 패스워드기호보드에 나열된 다수의 기호들이 매칭될 때 매칭된기호모임을 생성하여 인증처리수단으로 입력하는 매칭기호처리수단; 인증기준정보를 저장하

는 메모리 및; 인증기준정보에 기초하여 입력된 매칭된기호모임에 포함된 실상매칭기호에 실상 패스워드기호가 매칭되었는가를 판단하여 사용자의 메인 시스템으로의 접근을 허용 또는 거부하는 인증처리를 수행하는 인증처리수단을 포함한다.

<17> 본 발명의 다른 특징에 의하면, 패스워드 시스템의 사용자 인증 방법은: 매칭에 기준이 되는 하나의 실상매칭기호와 이를 위장하기 위한 다수의 허상매칭기호를 포함하는 제1 기호모임, 실상매칭기호와 매칭되어야 하는 하나의 실상패스워드기호와 이를 위장하기 위한 다수의 허상패스워드기호를 포함하는 제2 기호모임을 생성하는 단계; 제1 기호모임을 표시하기 위한 매칭기호보드와 제2 기호모임을 표시하기 위한 패스워드기호보드를 표시수단으로 표시하는 단계; 매칭기호보드의 실상매칭기호와 패스워드기호보드의 실상패스워드기호를 매칭수단에 의해 매칭시키는 것으로 패스워드를 입력하는 단계; 매칭기호보드와 패스워드기호보드의 기호들이 매칭되면 매칭된기호모임을 생성하여 인증처리수단으로 입력하는 단계 및; 인증처리를 위한 인증기준정보와 입력된 매칭된기호모임에 기초하여 사용자의 메인 시스템으로의 접근을 허락 또는 거부하는 인증처리 단계를 포함한다.

<48> (실시예)

<49> 본 발명은 패스워드 입력 과정이 타인에게 노출된다 하더라도 관찰자가 입력되는 패스워드를 감지할 수 없게 하는 새로운 패스워드 입력 방법과 이를 위한 사용자 인터페이스 그리고 이에 적합한 패스워드 인증 프로세스를 갖는 패스워드 시스템을 제공한다. 아래에서 설명되는 실시예들은 본 발명을 보다 잘 이해하기 위한 것일 뿐이며 본 발명이 아래의 실시예들로 한정되는 것으로 이해되서는 안 될 것이다. 이 분야의 통상적인 기술자들은 본 발명이 패스워드 입력을 요구하는 어떠한 장치나 방법에도 적용 될 수 있음을 잘 알 수 있을 것이다.

실시예의 설명에 있어서, 먼저 패스워드 노출을 방지할 수 있는 패스워드 입력 방법을 설명하고, 두 번째로 본 발명의 패스워드 입력에 해당하는 투-패스워드의 정의와 이로부터 실상매칭기호모임과 실상패스워드기호모임을 유도하는 방법을 설명한다. 세 번째로 본 발명의 패스워드 입력 방법에 적합한 사용자 인터페이스에 대하여 설명하고, 그리고 네 번째로 이러한 패스워드 입력 방법을 채용한 패스워드 시스템과 이의 패스워드 인증 프로세스를 설명한다. 각 실시예에서 동일한 구성이나 방법들에 대해서는 동일한 참조기호를 사용하고 그들의 반복적인 설명은 생략한다. 이하 본 발명의 바람직한 실시예들을 첨부된 도면들을 참조하여 상세히 설명한다.

51> 1. 패스워드 노출을 방지하기 위한 패스워드 입력 방법

52> 본 발명에 따른 패스워드 입력 방법은 사용자가 적어도 두 개 이상의 기호를 소정의 매칭 규칙에 따라 매칭시키고, 이러한 매칭 과정을 적어도 한 번 이상 반복하는 것으로서 패스워드 입력이 이루어진다. 그리고 패스워드 입력을 위해 매칭된 특정 기호쌍을 위장하기 위해 적어도 하나 이상의 다른 기호들의 허위 매칭이 동시에 이루어진다. 이와 같이, 다수의 기호들이 동시에 혼재되어 매칭됨으로 어느 것이 패스워드 입력을 위한 진정한 기호 매칭인지 관찰자가 판단할 수 없게 하여 패스워드 노출을 방지한다.

<53> 도 1a 및 도 1b는 본 발명의 패스워드 입력 방법을 설명하기 위한 도면으로, 도 1a에는 매칭전의 숫자열이 도 1b에는 매칭후의 숫자열이 각각 도시되어 있다. 도면을 참조하여, 상단에 다

수의 숫자들이 나열된 제1 숫자열(1)과 하단에 다수의 숫자들이 나열된 제2 숫자열(3)이 있다. 여기서 제1 숫자열(1)에 나열되는 숫자열은 그 순서가 순차적이고, 제2 숫자열(2)에 나열되는 숫자열은 그 순서가 비순차적으로 할 수 있다. 기호들의 나열 방법에 대한 구체적인 설명은 사용자 인터페이스를 설명하는 과정에서 상세히 설명한다. 그리고 기호열로 표시된 제1 숫자열(1)과 제2 숫자열(3)은 디스플레이 장치에 표시되는 그래픽 사용자 인터페이스(graphic user interface)의 한 형태로 표시될 수 있다.

<54> 사용자는 제1 숫자열(1)에 존재하는 하나의 특정 숫자와 제2 숫자열(3)에 존재하는 또 다른 하나의 특정 숫자를 소정의 매칭 규칙에 따라 매칭시키는 것으로서 패스워드를 입력한다. 매칭 규칙은, 예를 들어, 제1 숫자열(1)과 제2 숫자열(3)의 특정 숫자를 동일한 수직열로 정렬시키는 것이다.

<55> 패스워드 입력을 위해 매칭되어야 하는 숫자가 제1 숫자열(1)의 '3'과 제2 숫자열(3)의 '5'라고 할 때, 도 1a에 도시된 바와 같이, 매칭전 상태에서 제1 숫자열(1)의 '3'과 제2 숫자열(3)의 '5'는 서로 수직으로 정렬되어 있지 않다. 도면에서 제1 숫자열(1)의 '3'과 제2 숫자열(3)의 '5'를 특별히 해칭 표시한 것은 단지 상세한 설명의 이해를 위한 것이며 실재적인 사용자 인터페이스에서 보일 때에는 다른 기호들과 동일한 형태로 표시된다.

<56> 패스워드 입력을 위해 사용자는 제2 숫자열(3)을 네 번 우순환(또는 다섯 번 좌순환) 이동시켜, 도 1b에 도시된 바와 같이, 제1 숫자열(1)의 '3'과 제2 숫자열(3)의 '5'를 동일한 수직열에 위치시킨다. 이때, 제1 숫자열(1)과 제2 숫자열(3)에서 수직열로 매칭되는 숫자쌍들(5)은 순차적으로 '(1, 2)', '(2, 9)', '(3, 5)', '(4, 7)', '(5, 6)', '(6, 1)', '(7, 3)', '(8, 4)', '(9, 8)'로서 총 아홉 개가 발생된다. 이들 모두는 제2 숫자열(3)을 네 번 우순환 이동시킬

때 얻어지는 숫자쌍들이다. 그러나 패스워드 입력을 위해 실재 매칭된 숫자쌍은 '(3, 5)'이고 나머지 여덟 개의 허위 매칭된 숫자쌍들은 실재 매칭된 숫자쌍 '(3, 5)'를 위장시키기 위한 것이다.

<57> 이와 같은 기호 매칭은 한번의 패스워드 인증과정에서 적어도 한번 이상 반복적으로 수행된다. 그럼으로 비록 패스워드 입력 과정이 타인에게 노출된다 하더라도 타인은 입력된 패스워드(실재 매칭된 기호쌍)가 무엇인지를 인식할 수 없다. 후술되겠지만, 인증처리수단(미도시)은 매칭된 기호쌍들에 기초하여 패스워드 인증을 수행한다.

<58> 도 2는 본 발명의 패스워드 입력 방법을 집합 개념으로 일반화하여 설명하기 위한 개념도이다. 도면을 참조하여, 각기 n(n은 자연수)개의 기호들을 원소로 갖는 집합 A와 B가 있을 때 사용자는 패스워드 입력을 위해 집합 A의 특정된 하나의 원소와 집합 B의 특정된 하나의 원소를 선택하여 상호 매칭시킨다. 그리고 이 때 두 집합 A와 B의 각기 다른 원소들도 소정의 매칭 규칙에 의해 상호 매칭된다.

<59> 두 집합 A와 B의 특정된 두 원소를 매칭시키기 위한 방법의 일 예로서 상술한 숫자열의 예에서와 같이 어느 한 집합에 속한 원소들의 나열 순서를 변경하는 방법이 사용될 수 있다. 예를 들어, 집합 B의 원소들의 나열 순서를 변경한다. 나열 순서가 변경된 집합 B'와 집합 A간에 존재하는 소정의 매칭 규칙에 따라 매칭된 기호들의 집합 C가 생성된다.

<60> 이러한 기호들의 매칭 방법을 패스워드 입력 프로세스에 따라 설명하면 다음과 같다. 먼저, 단계 S1에서 집합 A와 집합 B의 각 원소들이 제공된다. 단계 S2에서는 집합 B의 원소들의 나열 순서를 변경시킨다. 단계 S3에서는 집합 A와 집합 B'의 원소들이 매칭 규칙에 따라 매칭된

기호쌍들의 집합 C가 생성된다. 인증처리수단(미도시)은 생성된 집합 C에 기초하여 인증처리를 수행한다.

<61> 여기서, 매칭에 기준이 되는 집합 A의 특정 원소를 실상매칭기호(real matching symbol; RMS)라고 하고, RMS를 위장하기 위한 나머지 기호들을 허상매칭기호(virtual matching symbol; VMS)라고 한다. RMS에 매칭시키기 위한 집합 B의 특정 원소를 실상패스워드기호(real password symbol; RPS)라고 하고, RPS를 위장하기 위한 나머지 기호들을 허상패스워드기호(virtual password symbol; VPS)라고 한다. 예를 들어, 첨부도면 도 3a에 도 1a에 도시된 숫자열에서 사용된 실상매칭기호와 허상매칭기호 그리고 실상패스워드기호와 허상패스워드기호가 각각 지적되어 표시되어 있다.

<62> 집합 A의 RMS와 집합 B'의 RPS가 매칭되면 집합 A의 VMS와 집합 B의 VPS들이 매칭되어진다. 집합 A와 집합 B'가 소정의 매칭 규칙에 의해 매칭된 집합 C의 기호쌍들을 매칭된기호모임(matched symbol group; MSG)이라 한다. 예를 들어, 도 3b에 도 1b에 도시된 매칭된 숫자열에서 매칭된 RMS와 RPS, 매칭된 VMS와 VPS 그리고 매칭된 기호 모임이 각각 지적되어 표시되어 있다.

<63> 한편, 한번의 패스워드 인증과정에서 상술한 RMS와 RPS의 매칭은 적어도 한번 이상 반복해서 이루어 질 수 있다. 첨부도면 도 4a 내지 도 4d에 다수의 기호 매칭 과정을 반복 수행하여 패스워드를 입력하는 예를 설명하기 위한 도면이 도시되어 있다. 도면에서 특별히 해칭 표시된 기호들은 단지 상세한 설명의 이해를 위한 것이며 실재적인 사용자 인터페이스에서 보여 질 때에는 다른 기호들과 동일한 형태로 표시된다. 기호열로 표시된 제1 숫자열(7)과 제2 숫자열(9)은 디스플레이 장치에 표시되는 그래픽 사용자 인터페이스의 한 형태로 표시될 수 있다.

<64> 각 도면에서 상위에 표시된 두 개의 숫자열은 매칭 전을 하위에 표시된 두 개의 숫자열은 매칭 후를 각각 표시하고 있다. 매칭 규칙은 제1 숫자열(7)의 RMS와 제2 숫자열(9)의 RPS를 동일한 수직열로 정렬시키는 것이다. 예를 들어, RMS가 '3','7','2','9'이고 RPS가 '5','1','6','6'인 경우 RMS와 RPS를 매칭시키기 위해서는, 도 4a 내지 도 4d에 도시된 바와 같이, 단계별로 표시되는 제1 숫자열(7)과 제2 숫자열(9)을 이용하여 '3'과'5', '7'과'1', '2'와 '6' 그리고 '9'와 '6'을 순차적으로 매칭시킨다.

<65> 다수의 RMS로 이루어진 기호들의 모임을 실상매칭기호모임(real matching symbol group; RMSG)이라 하고 다수의 RPS로 이루어진 기호들의 모임을 실상패스워드기호모임(real password symbol group; RPSG)이라 한다. 상술한 예에서 RMSG는 '3729'이고, RPSG는 '5166'이다.

<66> 이와 같은 본 발명의 패스워드 입력 방법은 하나의 RMS와 RPS가 매칭될 때 다수의 VMS와 VPS가 매칭되도록 하여 패스워드 입력을 관찰한 관찰자가 어느 기호 매칭이 RMS와 RPS의 매칭인지를 구분할 수 없도록 하여 패스워드 노출을 방지한다.

<67> 상술한 예에서, RMS와 VMS를 포함한 기호열의 기호들의 개수와 RPS와 VPS를 포함하는 기호열의 기호들의 개수가 동일(실시예에서는 9개로 동일함)하게 하였으나 서로 다르게 할 수도 있다. 예를 들어, 상위에 나열되는 기호열의 개수를 9개로하고 하위에 나열되는 기호열의 개수를 7개로 하는 등의 변형이 가능하다.

<68> 2. 투-패스워드와 이를 이용한 RMSG와 RPSG의 생성방법

<69> 본 발명의 패스워드 입력방법에 사용되는 패스워드는 기존 패스워드 시스템에서 사용되는 패스워드와 그 특징을 달리한다. 그럼으로 기존의 패스워드와 구분하기 위하여 본 발명의 패스워드 입력 방법에 사용되는 패스워드를 투-패스워드(two-password)라고 한다.

<70> 기존의 패스워드 시스템에 사용되는 패스워드는 기호들을 순차적으로 나열한 기호 모임이다. 그럼으로 패스워드 입력시 패스워드로 정의된 기호 모임을 정해진 순서에 따라 순차적으로 패스워드 시스템에 입력하면 되었다. 예를 들어, 신용카드의 패스워드를 '2976'으로 설정한 경우 신용카드를 이용하여 현금지급기를 사용하려면 현금지급기에 구비된 숫자 키패드를 이용하여 '2','9','7','6'을 순차적으로 입력한다.

<71> 그러나 본 발명의 패스워드 입력 방법에 사용되는 투-패스워드는 이러한 사용 방식을 갖는 종래의 패스워드와 그 특징이 다르다. 즉, 투-패스워드는 일부가 RMSG로 다른 일부가 RPSG로 구성될 수 있다. 또는 투-패스워드는 RMSG와 RPSG 중 어느 하나이고 그로부터 다른 하나를 유도할 수 있다. 이와 같이 서로 다른 두 개의 기호 모임인 RMSG와 RPSG로 구성할 수 있는 기호 모임이 투-패스워드인 것이다. 서로 다른 두 개의 기호 모임을 각기 제1 패스워드와 제2 패스워드라 할 수 있다. 구체적으로 투-패스워드로부터 RMSG와 RPSG를 생성하는 방법을 이하 첨부 도면 도 5a 내지 도 5d 그리고 도 6a 및 도 6b를 참조하여 구체적으로 설명한다.

<72> 먼저, 투-패스워드가 RMSG와 RPSG로 구성되는 일 예를 설명한다. 예를 들어, 투-패스워드가 '37295166'일 때 전단 네 개의 숫자'3729'를 RMSG로 하고, 후단 네 개의 숫자 '5166'을 RPSG로 할 수 있다. 이 경우 패스워드 입력을 위해 실상 매칭된 RMS와 RPS의 순서쌍은 '(3, 5)', '(7, 1)', '(2, 6)', '(9, 6)'이 된다. 이와 같은 투-패스워드로부터 RMSG와 RPSG를 생성하는

방법은 다음과 같이 일반화 할 수 있다. 첨부도면 도 5a에 도시된 바와 같이, 투-패스워드를 정의하는 경우 RMSG와 RPSG는 아래와 같으며 이때, RMS와 RPS의 순서쌍은 다음과 같이 일반화하여 표시할 수 있다.

73> 투-패스워드 : $X_1X_2X_3...X_{n-2}X_{n-1}X_nY_1Y_2Y_3...Y_{n-2}Y_{n-1}Y_n$ (n은 자연수)

74> RMSG : $X_1X_2X_3...X_{n-2}X_{n-1}X_n$

75> RPSG : $Y_1Y_2Y_3...Y_{n-2}Y_{n-1}Y_n$

76> RMS와 RPS의 순서쌍(RMS_i, RPS_i) : (X_i, Y_i) (1??i??n)

77> 두 번째로, 투-패스워드가 RMSG와 RPSG로 구성되는 다른 예로서, 투-패스워드로부터 교대적으로 선택된 숫자들의 모임을 각각 RMSG와 RPSG로 구성한다. 예를 들어, 투-패스워드가 '37295166'일 때 RMSG와 RPSG는 각각 '3256', '7916'으로 한다. 이 경우 패스워드 입력을 위해 실상 매칭된 RMS와 RPS의 순서쌍은 '(3, 7)', '(2, 9)', '(5, 1)', '(6, 6)'이다. 이와 같은 투-패스워드로부터 RMSG와 RPSG를 생성하는 방법은 다음과 같이 일반화 할 수 있다. 첨부도면 도 5b에 도시된 바와 같이, 투-패스워드를 정의하는 경우 RMSG와 RPSG는 아래와 같으며 이때, RMS와 RPS의 순서쌍은 다음과 같이 일반화하여 표시할 수 있다.

<78> 투-패스워드 : $X_1Y_1X_2Y_2X_3Y_3...X_{n-2}Y_{n-2}X_{n-1}Y_{n-1}X_nY_n$ (n은 자연수)

<79> RMSG : $X_1X_2X_3...X_{n-2}X_{n-1}X_n$

<80> RPSG : $Y_1Y_2Y_3...Y_{n-2}Y_{n-1}Y_n$

1> RMS와 RPS의 순서쌍 (RMS_i, RPS_i) : (X_i, Y_i) (1??i??n)

2> 세 번째로, 투-패스워드가 RMSG이고 이로부터 RPSG를 유도한다. 예를 들어, 투-패스워드가 '37295166'일 때 이 숫자 모임 전부를 RMSG로 사용하고 이로부터 RPSG를 유도한다. 유도 규칙은 예를 들어, RMSG를 1회 좌순환 하여 얻어지는 숫자 모임을 사용한다. 그럴 때 RPSG는 '72951663'이다. 이와 같을 때 패스워드 입력을 위해 실상 매칭된 RMS와 RPS의 순서쌍은 '(3, 7)', '(7, 2)', '(2, 9)', '(9, 5)','(5, 1)', '(1, 6)', '(6, 6)', '(6, 3)'이 된다. 이와 같은 투-패스워드로부터 RMSG와 RPSG를 생성하는 방법은 다음과 같이 일반화 할 수 있다. 첨부도면 도 5c에 도시된 바와 같이, 투-패스워드를 정의하는 경우 RMSG와 RPSG는 아래와 같으며 이때, RMS와 RPS의 순서쌍은 다음과 같이 일반화하여 표시할 수 있다.

83> 투-패스워드 : $X_1X_2X_3...X_{n-2}X_{n-1}X_n$ (n은 자연수)

84> RMSG : $X_1X_2X_3...X_{n-2}X_{n-1}X_n$

85> RPSG : $X_2X_3...X_{n-2}X_{n-1}X_nX_1$

86> RMS와 RPS의 순서쌍 (RMS_i, RPS_i) : (X_i, X_{i+1})(1??i??n-1), (X_i, X_1)(i=n)

87> 네 번째로, 투-패스워드의 일부가 RMSG이고 RMSG의 일부를 포함하는 또 다른 일부가 RPSG이다. 예를 들어, 투-패스워드가 '37295166'일 때 마지막 숫자를 제외한 나머지 모임 '3729516'을 RMSG으로 사용하고, 첫 번째 숫자를 제외한 나머지 모임 '7295166'을 RPSG으로 사용한다. 이와 같을 때 패스워드 입력을 위해 실상 매칭된 RMS와 RPS의 순서쌍은 '(3, 7)', '(7, 2)',

'(2, 9)', '(9, 5)','(5, 1)', '(1, 6)', '(6, 6)'이 된다. 이와 같은 투-패스워드로부터 RMSG와 RPSG를 생성하는 방법은 다음과 같이 일반화 할 수 있다. 첨부도면 도 5d에 도시된 바와 같이, 투-패스워드를 정의하는 경우 RMSG와 RPSG는 아래와 같으며 이때, RMS와 RPS의 순서쌍은 다음과 같이 일반화하여 표시할 수 있다.

<88> 투-패스워드 : $X_1X_2X_3...X_{n-2}X_{n-1}X_n$ (n은 자연수)

<89> RMSG : $X_1X_2X_3...X_{n-2}X_{n-1}$

<90> RPSG : $X_2X_3...X_{n-2}X_{n-1}X_n$

<91> RMS와 RPS의 순서쌍 (RMS_i, RPS_i) : $(X_i, X_{i+1})(1??i??n-1)$

<92> 상술한 바와 같이, 투-패스워드로부터 RMSG와 RPSG를 생성하는 방법은 다양하다. 상술한 예에서, 투-패스워드로부터 생성된 RMSG와 RPSG는 1:1 대응관계를 갖는다. 그러나 1:n 또는 n:1의 대응관계도 가질 수 있다. 예를 들어, 도 6a 및 도 6b에 도시된 바와 같이, 투-패스워드에서 RMSG로서 단 하나의 RMS만 생성하고 나머지 기호 모임을 RPSG로 생성하는 경우 그리고 그 역의 경우가 각각 그러하다. 이때, RMS와 RPS의 순서쌍은 각각 다음과 같이 일반적으로 표시할 수 있다.

<93> RMS와 RPS의 순서쌍 (RMS_i, RPS_i) : $(X_1, X_{i+1})(1??i??n-1)$

<94> RMS와 RPS의 순서쌍 (RMS_i, RPS_i) : $(X_i, X_n)(1??i??n-1)$

95> 이와 같이, 투-패스워드로부터 RMSG와 RPSG를 생성하는 방법과 RMS와 RPS의 순서쌍을 이루는 방법은 매우 많은 변형과 응용이 가능하다. 그러나 다양한 변형과 응용이라도 본 발명에 기초할 때 이 분야의 통상적인 기술자들에게는 자명한 것이며, 여기에 설명되지 않은 변형 및 응용의 경우라도 본 발명의 사상에 포함됨을 알 수 있을 것이다. 그리고 구체적인 설명은 생략하겠지만, 투-패스워드의 기본 정의를 응용하면 쓰리-패스워드(three-password)로 확장할 수 있고 더 나아가 포-패스워드(four-password) 및 그 이상으로도 확장이 가능함을 알 수 있다. 다만, 이러한 응용 및 확장은 패스워드를 사용하는 사용자의 입장을 고려하여야 할 것이다. 즉, 사용자가 투-패스워드를 암기하기 용이하여야 하고 투-패스워드를 입력하기 위해 기호들을 매칭하는 과정이 어렵지 않아야 한다.

96> 3. 투-패스워드 입력을 위한 사용자 인터페이스와 투-패스워드 시스템

97> 상술한 바와 같은 본 발명의 기호 매칭에 의한 패스워드 입력 방법은 그에 적합한 사용자 인터페이스에 의해서 구체화되어 제공된다. 그리고 나중에 설명되겠지만, 매칭된 기호쌍들에 기초하여 이루어지는 패스워드 인증 프로세스도 그에 적합하게 제공된다.

98> 도 7은 본 발명의 투-패스워드 시스템과 이를 채용한 메인 시스템과의 관계를 보여주는 블록도이다. 투-패스워드 시스템(30)은 사용자(10)가 투-패스워드를 입력하기 위한 사용자 인터페이스(20)를 제공한다. 사용자 인터페이스(20)는 사용자가(10)가 기호 매칭에 의해 투-패스워드를 입력할 수 있는 인터페이스 수단들을 구비한다. 투-패스워드 시스템(30)은 사용자로부터

입력되는 투-패스워드를 사용자 인터페이스(20)를 통해 받아들여 인증처리를 수행하며, 인가된 사용자에게 메인 시스템(40)으로의 접근을 허용한다.

[99] 사용자 인터페이스(20)는 후술하는 몇 가지의 실시예로 한정되는 것은 않으며, 이하 설명되는 사용자 인터페이스(20)의 구체적인 실시예들은 본 발명을 보다 잘 이해하기 위해 제공되어지는 것들이다. 그럼으로 투-패스워드 시스템(30)을 채용하게 되는 메인 시스템(40)의 특성에 따라 사용자 인터페이스(20)의 구체적인 구성들은 변형되어 적용될 수 있다.

[100] 예를 들어, 개인용 컴퓨터 시스템에 투-패스워드 시스템(30)이 탑재되는 경우 사용자 인터페이스(20)는 그래픽 사용자 인터페이스(graphic user interface)를 포함할 수 있으며, 전자적 도어락 시스템(electrical door lock system)에 탑재되는 경우에는 사용자 인터페이스(20)는 기계적 메커니즘과 전자 회로를 포함하는 형태로 구현될 수 있다.

[101] 구체적으로, 사용자 인터페이스(20)와 투-패스워드 시스템(30)의 구성을 설명한다. 도 8은 본 발명의 투-패스워드 시스템을 위한 사용자 인터페이스의 기본 구성을 보여주는 도면이고, 도 9는 본 발명의 투-패스워드 시스템의 인증 프로세스를 개략적으로 보여주는 플로우차트이다.

[102] 본 발명의 바람직한 실시예에 따른 투-패스워드 시스템(30)은 크게 표시제어수단(31), 기호발생수단(32), 매칭기호처리수단(33), 인증처리수단(34) 그리고, 메모리(35)를 포함하여 구성된다. 투-패스워드 입력을 위한 사용자 인터페이스(20)는 표시수단(22)과 매칭수단(24)을 포함한다.

[103] 도 8 및 도 9를 참조하여, 단계 S10에서 기호발생수단(32)은 표시수단(22)에 표시될 실상매칭기호(RMS), 허상매칭기호(VMS), 실상패스워드기호(RPS) 및 허상패

스워드기호(VPS)를 포함하는 기호들의 나열 순서인 기호모임을 생성하여 표시제어수단(31)으로 제공한다. 단계 S20에서 표시제어수단(31)은 제공된 기호모임을 표시수단(22)으로 출력하고, 표시수단(22)은 표시제어수단(31)의 제어를 받아 기호모임을 표시한다.

<04> 단계 S30에서 사용자(10)는 매칭수단(24)을 이용하여 표시수단(22)에 표시된 기호들을 매칭시키고, 단계 S40에서 매칭기호처리수단(33)은 매칭수단(24)을 통한 사용자의 입력에 기초하여 매칭된기호모임(MSG)을 생성하고, 단계 S50에서, 이를 인증처리수단(34)으로 입력한다. 단계 S60에서 인증처리수단(34)은 메모리(35)에 저장되어 있는 인증기준정보(36)에 기초하여 소정의 패스워드 인증처리를 수행한다. 이에 대한 구체적인 프로세스는 후술한다.

<05> 이와 같은 투-패스워드 시스템은 종래의 패스워드 시스템과 달리 투-패스워드를 입력하기 위한 기호모임을 생성하여 사용자에게 표시하는 과정이 선행된다. 그리고 매칭된기호모임(MSG)에 기초한 인증처리 과정 또한 종래의 패스워드 시스템과 그 특징이 다르다. 이들에 관한 구체적인 설명은 후술한다.

<106> 계속해서, 메인 시스템(40)에 따른 사용자 인터페이스(20)의 구체적인 실시예를 첨부도면 도 10 내지 도 18을 참조하여 설명한다.

<107> 도 10은 메인 시스템에 따른 사용자 인터페이스의 일 실시예를 보여주는 도면이다. 투-패스워드 시스템(20)이 그래픽 사용자 인터페이스를 갖는 시스템 예를 들어, 개인용 컴퓨터 시스템, PDA, ATM 금융단말기 등의 메인 시스템(40)에 탑재될 수 있다. 이때, 사용자 인터페이스(20)는 표시수단(22)으로서 CRT 디스플레이 장치, 액정 디스플레이 장치 등의 디스플레이장치(50)

와 이에 표시되는 그래픽 사용자 인터페이스(60) 또는 매칭수단(24)으로서 예컨대 키보드 장치, 포인팅 장치 등의 입력장치(54) 또는 이들의 조합으로 구성된다.

<8> 디스플레이 장치(50)의 화면(52)에 표시되는 그래픽 사용자 인터페이스(60)는 RMS와 VMS를 표시하기 위한 제1 기호보드(61)와 RPS와 VPS를 표시하기 위한 제2 기호보드(62)를 포함한다. 제1 기호보드(61)와 제2 기호보드(62)는 이하 각기 매칭기호보드(matching symbol board)와 패스워드기호보드(password symbol board)라고 한다. 사용자(10)는 투-패스워드를 입력하기 위해 입력장치(54)를 사용하며, 사용자(10)의 제어에 따라 매칭기호보드(61) 및/또는 패스워드기호보드(62)에 나열된 기호들이 순환 이동 표시된다.

<09> 순환 표시 방법은 예를 들어, 매칭기호보드(61)는 고정 표시되고, 패스워드기호보드(62)가 우순환 또는 좌순환 이동 표시될 수 있다. 그리고 매칭기호보드(61)에 나열되는 기호열은 매칭에 기준이 됨으로 빠르게 RMS을 발견할 수 있도록 나열 순서가 순차적으로 일정하게 고정 표시된다. 사용자가 충분히 RMS를 발견할 수 있을 정도의 복잡도를 갖는다면 매칭기호보드(61)의 기호 나열 순서를 비순차적으로 랜덤하게 표시할 수도 있을 것이다. 패스워드기호보드(62)에 나열되는 기호들은 비복원 랜덤하게 표시하는 것이 바람직하다.

<110> 순환 표시의 다른 방법으로는 매칭기호보드(61)와 패스워드기호보드(62)가 각기 서로 다른 방향으로 순환 표시될 수 있다. 또는 매칭기호보드(61)는 고정 표시되고 패스워드기호보드(62)에 나열된 각 숫자들이 제자리에서 상방향 또는 하방향으로 증가되거나 감소되면서 순환 표시되도록 할 수도 있다.

<111> 이러한 순환 표시의 방법은 설명된 방법 외에도 다양한 응용이나 변형이 있을 수 있을 것이며, 이러한 응용이나 변형은 이 분야의 기술자들에게는 본 발명에 기초하여 자명한 것이다.

2> 기호열의 표시 형태에 있어서, 도시된 바와 같이, 매칭기호보드(61)와 패스워드기호보드(62)는 일자로 나열된 표시 형태뿐만 아니라 그 외에도 다양한 표시 형태를 가질 수 있다. 예를 들어, 도 11a 내지 도 11d에 도시된 바와 같이, 원형, 매트릭스 형태를 가질 수 있다. 그리고 나열되는 기호들은 숫자 뿐만 아니라 문자, 도형, 그림과 이들의 조합 등 기호화 될 수 있는 어떠한 수단들도 가능하며, 사용자의 기호인식을 도울 수 있도록 색(color)이 더불어 표시될 수 있다. 예를 들어, 패스워드기호보드(62)에 표시되는 숫자들이 포함된 원형 안에 각기 다른 색을 표시할 수 있다. 색을 선택하는 방법은 사용자가 기호인식을 빠르게 할 수 있도록 한다. 이와 같은 기호의 표시 방법은 다양한 많은 응용이 존재할 수 있으며 이 분야의 기술자들에게는 본 발명에 기초할 때 자명한 것이다.

13> 매칭기호보드(61)와 패스워드기호보드(62)에서 어느 하나의 기호보드가 나열 순서가 연상 가능하도록 고정 표시되는 경우 그 표시를 생략할 수 있다. 예를 들어, 매칭기호보드(61)에 1~9까지의 숫자가 순차적으로 나열되어 표시되는 경우 사용자는 매칭기호보드(61)를 쉽게 연상할 수 있음으로, 도 12에 도시된 바와 같이, 그 표시를 생략할 수 있다.

114> 다른 실시예로서, 매칭기호보드 및 패스워드기호보드(61, 62)는 도 13에 도시된 바와 같이, 그 표시 형태를 상호 교환된 형태로 표시할 수 있다. 예들 들어, 패스워드기호보드(62)에 나열되는 기호들의 순서를 순차적으로 하고, 매칭기호보드(61)에 나열되는 기호들의 순서를 비복원 랜덤으로 할 수 있다. 또는 패스워드기호보드(62)를 고정 표시하고, 매칭기호보드(61)를 사용

자의 제어에 따라 순환 표시할 수 있다. 이러한 변경은 이 분야의 기술자들에게는 본 발명에 기초할 때 자명한 것이다. 또 다른 실시예로서, 도 14에 도시된 바와 같이, 패스워드기호보드(62)에 표시되는 기호 열이 두 개 이상 동시에 표시되도록 할 수 있다. 사용자는 패스워드기호보드(62)에 표시되는 각각의 기호열을 이용하여 매칭기호보드(61)와 순차적으로 기호매칭을 함으로서 투-패스워드를 입력한다. 패스워드기호보드(62)에 표시되는 다수의 기호열의 개수는 RPSG의 개수만큼 표시할 수 있다.

<15> 한편, 상술한 예에서는 기호 매칭을 위해 기호열을 순환 이동시켰으나, 또 다른 실시예로서 기호열의 순환 이동량을 직접 입력하도록 할 수 있다. 도 15에 도시된 바와 같이, 그래픽 사용자 인터페이스(60)에 별도의 입력창(63)을 두고 사용자가 패스워드기호보드(62)의 순환 이동량을 직접 입력하도록 할 수 있다. 예를 들어, RMSG가 하나의 RMS로서'3'이고 RPSG가 '5618'인 경우 매칭기호보드(61)에 표시된 기호 '3'을 기준으로 하여 패스워드기호보드(62)의 '5', '6', '1', '8'을 우순환시켜 매칭시킬 때 각각 순환 이동량은 4회, 2회, 1회, 7회이다. 그럼으로 입력창(63)에 '4217'을 입력한다.

<16> 도 16에 도시된 바와 같이, 기호열을 순환 매칭시키기 위한 다수의 매칭제어버튼(64)을 그래픽 사용자 인터페이스(60)에 구비할 수도 있다. 매칭제어버튼(64)은 예를 들어, 좌우순환이동버튼, 시작/리셋버튼, 매칭버튼, 입력완료버튼을 구비한다.

<17> 또 다른 실시예로서, 매칭기호보드(61) 또는 패스워드기호보드(62)가 자동으로 순환하고 사용자는 매칭기호보드(61)의 RMS와 패스워드기호보드(62)의 RPS가 매칭될 때 이를 알리기 위한 입

력만을 하도록 할 수 있다. 예를 들어, 도 17에 도시된 바와 같이, 패스워드기호보드(62)가 자동 순환할 때 사용자는 그래픽 사용자 인터페이스(60)에 표시되는 엔터버튼(65)을 입력하여 기호가 매칭되었음을 알리거나 입력장치(54)의 엔터-키를 사용할 수 있다.

118> 이상에 설명한 그래픽 사용자 인터페이스는 설명된 실시예들만으로 한정되는 것은 아니며, 상술한 실시예들을 두 가지 이상 혼합하여 사용도 가능하다. 그리고 매칭기호보드 및 패스워드 기호보드(61, 62)에 나열되는 기호들의 개수도 사용자 입장과 보안성을 고려하여 적절한 개수로 설정할 수 있다. 예를 들어, 보안성을 높이고자 하는 경우 나열되는 기호들의 개수를 증가할 수 있으며, 신속한 패스워드 입력과 처리가 요구되는 경우에는 나열되는 기호들의 개수를 감소할 수 있을 것이다.

119> 본 발명의 투-패스워드 시스템은 기계적 메커니즘과 이와 관련된 전자 회로를 갖는 시스템 예를 들어, 전자적 도어락(electrical doorlock)과 같은 잠금 시스템(locking system), 출입 통제 시스템(entrance control system) 등에 탑재될 수 있다. 투-패스워드 시스템은 메인 시스템에 탑재되는 기계적 메커니즘과 전자 회로와 연동하여 동작할 수 있으며, 이 경우 사용자 인터페이스는 다음과 같이 구성될 수 있다.

120> 도 18은 전자 회로와 연동한 투-패스워드 시스템의 사용자 인터페이스의 일 예를 보여주는 도면이고, 도 19는 하나의 기호보드만을 표시하는 변형예를 보여주는 도면이다. 그리고 도 20은 도 18의 사용자 인터페이스의 회로 구성의 일 예를 보여주는 도면이다.

<1> 도면을 참조하여, 패스워드 입력패널(password input panel)(70)은 예를 들어, 전자적 도어락 또는 출입 통제 시스템과 같은 메인 시스템(40)의 투-패스워드를 입력하기 위한 사용자 인터페이스로 제공된다. 패스워드 입력패널(70)은 기호 모임을 표시하기 위한 표시수단으로서 LCD(71)를 구비한다. LCD(71)에는 RMS와 VMS를 표시하기 위한 매칭기호보드(72) 그리고 RPS와 VPS를 표시하기 위한 패스워드기호보드(73)의 이미지가 표시된다. 그러나 도 19에 도시된 바와 같이, LCD(71)에는 패스워드기호보드(73)만을 표시하고, 패스워드 입력 패널(70)의 전면 상부에 매칭기호보드 표시영역(72a)을 마련하여 기호들을 인쇄 표시할 수도 있다. 그리고 매칭 수단으로서 패스워드 입력 패널(70)의 전면에 다수 개의 매칭제어버튼(74)이 구비된다. 메칭 제어버튼(74)으로 예를 들어, 좌우순환이동버튼, 시작/리셋버튼, 매칭버튼, 입력완료버튼이 구비된다.

<22> 패스워드 입력패널(70)은 LCD 제어회로 및 버튼입력 처리회로(75)를 구비하여 투-패스워드 시스템(30)으로부터 제공되는 표시제어신호에 응답하여 LCD(71)에 매칭기호보드 및 패스워드기호보드(72, 73)를 표시한다. 사용자는 매칭제어버튼(74)을 이용하여 투-패스워드를 입력한다. LCD 제어회로 및 버튼입력 검출회로(75)는 매칭제어버튼(74)의 입력을 받아들여 투-패스워드 시스템(30)으로 제공한다.

<123> 도 21은 기계적 메커니즘과 연동한 투-패스워드 시스템의 사용자 인터페이스의 일 예를 보여주는 도면이고, 도 22는 도 21의 사용자 인터페이스의 회로 구성의 일 예를 보여주는 도면이다.

<124> 도면을 참조하여, 패스워드 입력패널(80)은 전면 상단에 매칭기호보드 표시영역(81)이 마련되어 RMS와 VMS를 표시하는 기호들이 인쇄 표시된다. RPS와 VPS를 표시하기 위한 패스워드기호

보드는 다수의 휠(83)이 결합된 휠-메커니즘(82)으로 구성된다. 각각의 휠(83)에는 다수의 기호가 순환 인쇄되어 있다.

<5> 패스워드 입력패널(80)은 휠 구동 및 회전량 검출회로(85)를 구비하여 투-패스워드 시스템(30)으로부터 제공되는 표시제어신호에 응답하여 휠-메커니즘(82)을 구동한다. 사용자는 휠제어버튼(74)을 이용하여 투-패스워드를 입력한다. 휠제어버튼(74)은 휠-메커니즘(82)을 상하 회전 동작시키기 위한 휠과 매칭 입력 신호를 발생하는 버튼이 결합된 구조를 갖는다. 휠 구동 및 회전량 검출회로(85)는 휠제어버튼(84)의 입력을 받아들여 투-패스워드 시스템(30)으로 제공한다.

<26> 이와 같은 휠 메커니즘(82)을 이용한 투-패스워드 시스템의 사용자 인터페이스는 상술한 그래픽 사용자 인터페이스로도 구현이 가능하다. 즉, 매칭기호보드 및/또는 패스워드기호보드를 그래픽 사용자 인터페이스로서 표시하되 순환 이동 방식을 상하 순환 이동 방식으로 구현할 수 있으며, 이 때 상하 순환 이동의 제어는 입력 장치나 화면에 별도의 휠제어버튼을 표시하고 이를 이용하도록 할 수 있다.

<27> 이상에서 설명한 바와 같이, 본 발명의 투-패스워드 시스템의 투-패스워드 입력을 위한 사용자 인터페이스는 메인 시스템(30)의 특성에 따라 다양하게 구성될 수 있다. 본 실시예에서 언급되지 않은 다른 사용자 인터페이스 방식이라도 본 발명에 기초할 때 이 분야의 통상의 기술자들은 기호 매칭에 의한 패스워드 입력 방식을 채용할 수 있을 것이다.

<28> 4. 투-패스워드 시스템의 인증 프로세스

9> 도 8 및 도 9를 참조하여 개략적으로 설명한 투-패스워드 시스템의 인증 프로세스에 관한여 단계 별로 보다 구체적으로 설명한다.

0> 도 8 및 도 9를 참조하면, 투-패스워드 인증 프로세스의 단계 S10에서 기호발생수단(32)은 표시수단(22)에 표시될 기호 모임을 생성한다. 기호발생수단(32)은 매칭기호보드와 패스워드기호보드에 나열되는 기호들을 생성함에 있어서 각기 그 순서를 비복원 램덤하게 하거나 또는 정해진 순서를 갖도록 생성할 수 있으며 이들을 혼합하여 사용할 수 있다.

31> 예를 들어, 매칭기호보드에 나열될 기호는 정해진 순서로, 패스워드기호보드에 나열될 기호는 비복원 랜덤하게 생성할 수 있다. 또는 매칭기호보드와 패스워드기호보드를 모두 비복원 랜덤하게 생성할 수 있다. 또는 패스워드기호보드에 나열될 기호들은 비복원 랜덤하게 생성하고, 매칭기호보드에 나열될 기호들은 패스워드기호보드에 나열된 기호들의 순서를 회전하여 생성할 수 있다.

32> 다른 예로, 메모리(35)에 저장된 인증기준정보(36)에 기초하여 RMSG과 RPSG를 추출하고 이에 기초하여 기호들의 나열 순서를 결정하되 사용자가 투-패스워드를 입력하기 편리한 순서로 기호들의 나열 순서를 결정할 수 있다. 예를 들어, 패스워드기호보드의 회전수를 소정의 범위 이내가 되도록 하기 위해 기호들의 나열 순서를 결정할 수 있다.

133> 첨부 도면 도 23에 패스워드기호보드의 회전수를 소정의 범위 이내가 되도록 위한 기호 나열의 일 예를 보여주는 도면이 도시되어 있다. 패스워드기호보드(62)가 자동으로 우순환 하는 경우에 투-패스워드가 '134672'이고, RMSG가 '147' RPSG가 '362'인 경우에 패스워드기호보드(62)에 나열되는 기호를 '378612954'로 생성한다. 그리고 세 번의 기호 매칭에서 패스워드기호보드(62)는 동일한 순서로 기호들이 나열된다. 그러면 초기 표시 상태에서 '1'과 '3', '4'와 '6'은 이미 매칭되어 표시됨으로 엔터버튼(65)을 두 번 입력하는 것으로 '1'과 '3', '4'와 '6'이

매칭되고, 그 후 패스워드기호보드(65)가 오른쪽으로 한 칸 이동하면 '7'과 '2'가 매칭됨으로 그 때 엔터버튼(65)을 입력하면 된다. 이와 같이, 사용자의 편리를 위해 기호들의 나열 순서가 결정될 수 있다.

<134> 그러나, 모든 기호 매칭에 있어서 기호의 순환 이동이 전혀 없도록하는 것은 제외해야할 것이다. 모든 기호 매칭을 엔터버튼(65)만 입력하다면 보안성이 취약해질 수 있음으로, 보안성을 고려하여 적어도 한번 이상은 순환 이동이 있도록 해야 할 것이다. 즉, 지나친 순환 이동이 발생되지 않으면서 보안성도 확보할 수 있는 기호 나열이 이루어지도록 해야 한다. 여기서 중요한 것은 사용자가 투-패스워드를 입력함에 있어서 최대한 입력의 편리성을 제공하는데 있다.

<135> 한편, 투-패스워드 시스템의 인증 프로세스에서는 투-패스워드의 입력과 함께 사용자에게 부여된 고유의 ID를 입력하는 단계를 포함할 수 있다. 예를 들어, 메인 시스템(40)이 사용자 수가 다수인 시스템인 경우 사용자의 ID를 별도로 입력하는 것이 필요하다. 이에 대한 구체적인 설명은 후술한다. 사용자가 별도의 ID를 입력하는 인증 프로세스에서는 입력된 ID를 이용하여 메모리(35)로부터 인증기준정보(36)를 추출하여 상술한 바와 같은 기호 생성 단계를 수행할 수 있다.

<136> 이상과 같은 기호 나열 순서를 결정하여 기호모임을 생성하는 과정은 투-패스워드의 입력 과정에서 한번만 생성될 수 도 있고 또는 기호 매칭시마다 반복적으로 수행될 수 있다.

<137> 이와 같이 생성된 기호 모임은 표시제어수단(31)으로 제공되고 단계 S20에서 표시제어수단(31)은 생성된 기호모임을 표시수단(22)으로 출력한다. 표시수단(20)은 표시제어수단(31)의 제어

를 받아 기호모임을 표시한다. 기호 모임을 표시하는 방법은 상술한 투-패스워드 입력을 위한 사용자 인터페이스의 다양한 실시예들 중 어느 하나로 표시된다.

<38> 단계 S30에서 사용자(10)는 매칭수단(24)을 이용하여 표시수단(22)에 표시되는 기호들을 매칭시킨다. 단계 S40에서 매칭기호처리수단(33)은 매칭수단(24)을 통한 사용자의 입력에 기초하여 매칭된기호모임(MSG)을 발생한다. MSG의 발생예를 첨부도면 도 24a 내지 도 24d를 참조하여 설명한다.

<39> 도면을 참조하여, 매칭기호보드(90)와 패스워드기호보드(91)에서 특별히 해칭 표시된 기호들은 단지 상세한 설명의 이해를 위한 것이며 실재적인 사용자 인터페이스에서 보여 질 때에는 다른 기호들과 동일한 형태로 표시된다.

<40> RMS가 '3','7','2','9'이고 RPS가 '5','1','6','6'인 경우 사용자는, 도면에 도시된 바와 같이, 매칭 단계별로 매칭기호보드(90)와 패스워드기호보드(91)의 '3'과'5', '7'과'1', '2'와 '6' 그리고 '9'와 '6'을 순차적으로 매칭시킨다. 이때, 생성되는 MSG는 도 25에 도시된 바와 같다. 매 단계별로 생성되는 MSG(MSG_1~MSG_4)는 단계 S50에서 인증처리수단(34)으로 입력된다.

<41> 여기서, 매칭기호보드(90)에 나열된 기호들의 순서가 정해져 있는 경우 매칭된 시점에서 패스워드기호보드(91)에 나열된 기호들만을 인증처리수단(34)으로 전송할 수 있다. 여기서, 첫 번째 매칭된 경우에 대해서만 패스워드기호보드(91)에 나열된 기호들의 모든 정보가 전송되고 두 번째 매칭 후부터는 패스워드기호보드(91)가 몇 번 회전하였는가 하는 정보만 전송할 수도 있

다. 그리고 매칭기호보드(90)에 있는 기호들의 순서가 정해져 있지 않은 경우 매칭 시점에서 매칭기호보드(90)와 패스워드기호보드(91)에 있는 모든 기호들을 순서별로 전송할 수 있다.

2> 이와 같이, 인증처리수단(34)으로 전송되는 정보는 사용자 인터페이스의 특징에 따라 다양한 변형과 응용이 있을 수 있으며, 이러한 변형과 응용은 본 발명에 기초할 때 이 분야의 통상적인 기술자들에게는 자명한 것이다. 그리고 인증처리수단(34)으로 전송하는 시점은 모든 투-패스워드 입력이 완료된 시점에서 한 번에 이루어 질 수 있고, 또는 하나의 매칭이 이루어 질 때마다 전송이 이루어 질 수도 있다.

43> 단계 S60에서 인증처리수단(34)은 메모리(35)에 저장된 인증기준정보(36)에 기초해서 소정의 패스워드 인증처리를 수행한다. 패스워드 인증처리의 구체적인 프로세스를 보여주는 플로우차트가 첨부도면 도 26에 도시되어 있다.

44> 도 26을 참조하여, 인증처리수단(34)은 단계 S61에서 MSG를 입력 받는다. 단계 S62에서 메모리(35)로부터 인증기준정보(36)를 패치한다. 이 실시예에서, 인증기준정보는 투-패스워드이다. 단계 S63에서 투-패스워드로부터 RMSG와 RPSG를 유도한다. 단계 S64에서 투-패스워드로부터 유도된 RMSG와 매칭되는 기호들을 MSG에서 결정한다. 예를 들어, 도 27에 도시된 바와 같이, RMSG가 '3729'인 경우 이와 매칭되는 MSG의 기호들은 '5','1','6','6'으로 결정된다.

145> 단계 S65에서 MSG에서 결정된 기호모임과 투-패스워드에서 유도된 RPSG를 비교하고, 단계 S66에서 두 기호들이 일치하는가를 판단한다. 일치하는 경우 단계 S67에서 시스템 접근을 허락하고, 일치하지 않는 경우에는 단계 S68에서 시스템 접근을 거부한다.

6> 여기서, 메모리(35)에 저장된 인증기준정보(35)는 상술한 예에서와 같이 투-패스워드일 수도 있으나, RMSG와 RPSG로 구분되어 각기 저장되거나 어느 하나만 저장될 수 있다. 어느 하나만 저장된 경우에는 저장된 정보로부터 다른 하나의 정보를 유도한다. 예를 들어, 도 5c에 도시한 바와 같이 RMSG와 RPSG를 구성하는 경우 RMSG를 저장하고 RPSG는 유도하여 사용할 수 있다. 후술되겠지만, 인증 프로세스에서 사용자 ID를 입력하는 경우 입력된 ID에 기초하여 메모리(35)로부터 인증기준정보(36)를 패치(patch)할 수 있다.

47> 한편, 상술한 투-패스워드 시스템의 인증 프로세스는 단일 사용자 시스템에 적용 가능한 예로서, 복수 사용자 시스템의 경우에는 투-패스워드 입력과 함께 사용자 ID를 입력하는 단계를 더 포함한다. 도 28에 도시된 바와 같이, 인증처리수단(34)은 입력된 사용자 ID에 기초하여 메모리(35)에 저장된 해당 인증 기준 정보(37)를 패치한다.

148> 복수 사용자 시스템의 경우, 별도의 사용자 ID를 입력하는 과정 없이 인증 프로세스가 처리될 수 있다. 예를 들어, 도 29에 도시된 바와 같이, 입력된 MSG를 인덱스로 활용하는 경우가 그것이다. 여기서, 기호발생수단(32)은 MSG를 이용하여 인증기준정보를 패치한다. 사용자 ID를 입력하는 방법은 입력 장치를 사용하여 직접 입력하는 방법이나, 그래픽 사용자 인터페이스에서 버튼을 이용하는 방법을 사용할 수 있다. 또한, 단일 사용자 시스템이라도 사용자 ID를 입력하는 과정은 포함될 수 있다.

149> 5. 투-패스워드 시스템의 응용

0> 본 발명의 투-패스워드 시스템은 패스워드 입력이 요구되는 어떠한 시스템에도 적용이 가능하다. 예를 들어, 상술한 예에서와 같이, 개인용 컴퓨터 시스템, 잠금 시스템, ATM 금융 단말기, PDA, 셀룰러폰, 인터넷 뱅킹 시스템, 사이버 트레이딩 시스템 등 그 응용 분야는 다양하다.

51> 본 발명의 투-패스워드 시스템(30)이 스탠드얼론 시스템(standalone system)(100)에 탑재되는 경우의 일 예를 보여주는 도면이 도 30에 도시되어 있다. 스탠드얼론 시스템(100)에 탑재된 투-패스워드 시스템(30)의 사용자 인터페이스(20)는 시스템에 내장되거나 혹은 외장 형태를 가질 수 있다. 예를 들어, 개인용 컴퓨터 시스템의 경우, 상술한 예에서와 같이, 그래픽 사용자 인터페이스 또는 입력장치 또는 이들의 조합으로 구성될 수 있다.

152> 도 31은 본 발명의 투-패스워드 시스템이 네트워크 환경에서 메인 시스템에 탑재되는 경우의 일 예를 보여주는 도면이고, 도 32는 네트워크 환경에서 투-패스워드 시스템이 통신 단말기에 탑재되는 경우의 일 예를 보여주는 도면이다.

153> 본 발명의 투-패스워드 시스템은 네트워크 환경에서 이용될 수 있다. 투-패스워드 시스템(30)은, 도 31에 도시된 바와 같이 통신망(120)을 통해 연결된 메인 시스템(40)에 탑재될 수 있다. 통신 단말기(110)는 통신망(120)을 통해 메인 시스템(40)으로부터 기호모임 정보를 제공받아 사용자 인터페이스(20)를 통해 표시하고, 사용자는 사용자 인터페이스(20)를 사용하여 투-패스워드를 입력한다. 투-패스워드 입력에 의해 발생되는 정보 예를 들어, 매칭된기호모임(MSG)은

통신 단말기(110)에 의해 통신망(120)을 통해 메인 시스템(40)에 탑재된 투-패스워드 시스템(30)으로 입력된다. 또는 통신 단말기(110)에서 메인 시스템(40)으로 전송되는 정보는 기호 매칭시 기호열의 순환 이동량만이 전송될 수도 있다.

[54] 전송되는 정보는 필요에 따라 암호화 처리되거나 공개 키 기반구조와 같은 보안 플랫폼들과 결합되어 사용될 수 있다. 여기서 전송되는 정보에 사용자 ID 정보가 포함할 수 있다. 또는 상술한 예에서와 같이 MSG가 인덱스 기능을 겸하는 경우 즉, 사용자 ID를 나타내는 경우에는 MSG만 전송될 수 있으며 이외에도 다양한 응용은 가능하다.

[55] 한편, 통신 단말기(110)에 사용자 ID가 저장되어 있는 경우, 사용자는 투-패스워드만을 입력하고 별도의 ID 입력 과정은 생략될 수 있다. 이때, 메인 시스템(40)에 탑재된 투-패스워드 시스템(30)은 메모리에서 투-패스워드나 실상기호 모임과 패스워드 기호 모임을 패치하는 것은 통신 단말기(110)로부터 제공되는 사용자 ID를 이용할 수 있다.

[56] 다른 실시예로, 투-패스워드 시스템(30)은, 도 32에 도시된 바와 같이, 통신 단말기(110)에 탑재될 수 있다. 이 경우, 인증 프로세스는 통신 단말기(110)에서 이루어진다.

[57] 이상과 같은 본 발명의 투-패스워드 시스템(30)은 사용자 인터페이스(20)와, 도 8에 도시된 바와 같은, 구체적인 구성들은 스탠드 얼론 시스템(100)에 탑재되거나 유선, 무선, 컴퓨터 네트웍 등의 다양한 형태의 통신망(120)으로 상호 접속되는 통신 단말기(110)나 메인 시스템(40)에 탑재될 수 있으며 그 구성의 일부가 분리되어 구성될 수도 있다. 예를 들어, 인증기준정보(36)를 저장하기 위한 메모리(35)는 통신 단말기(110)에 구성되거나 또는 메인 시스템(40)에 구성될 수 있다.

58> 한편, 상술한 실시예에서는 기호들의 매칭만을 예로하여 설명하였으나, 본 발명의 매칭 방법은 퍼즐(puzzle)과 같이 하나의 그림을 완성하거나 특별한 숫자를 만들어 가는 과정이 투-패스워드의 입력일 수 있도록 응용할 수 있다.

59> 상술한 바와 같은, 본 발명의 투-패스워드 시스템의 구성 및 동작을 몇 가지의 실시예들로서 설명하였으나 이는 예를 들어 설명한 것에 불과하며 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 다양한 변화 및 변경이 가능하다는 것을 이 분야의 통상적인 기술자들은 잘 이해할 수 있을 것이다. 또한 각 실시예들은 하나 이상 복합적으로 적용되어 실시될 수 있음을 잘 알 수 있을 것이다.

【발명의 효과】

60> 이상과 같은 본 발명의 투-패스워드 시스템은 패스워드 입력 과정을 관찰한 타인에게 입력되는 패스워드가 무엇인지를 알 수 없게 한다. 즉, 사용자는 자신만이 알고 있는 투-패스워드를 입력하기 위하여 실상매칭기호와 실상패스워드기호를 매칭시키며, 이 때 다수의 허상매칭기호와 허상패스워드기호가 더불어 혼재되어 매칭됨으로 관찰자는 어느 매칭이 투-패스워드 입력을 위한 매칭인지를 알 수 없다. 그럼으로 패스워드 입력시 타인에게 입력 중인 패스워드가 노출되는 것이 방지되어, 사용자의 심리적 불안감을 해소할 수 있고, 시스템의 보안도를 향상시킬 수 있는 효과가 있다.

【특허청구범위】

【청구항 1】

매칭에 기준이 되는 하나의 실상매칭기호와 실상매칭기호를 위장하기 위한 다수의 허상매칭기호를 포함하는 다수의 기호들이 나열되어 표시되는 매칭기호보드, 실상매칭기호와 매칭되어야 하는 하나의 실상패스워드기호와 실상패스워드기호를 위장하기 위한 다수의 허상패스워드기호를 포함하는 다수의 기호들이 나열표시되는 패스워드기호보드를 표시하는 표시수단;

매칭기호보드와 패스워드기호보드에 표시될 기호모임을 생성하는 기호발생수단;

기호발생수단에서 생성된 기호모임에 대한 정보를 받아들여 매칭기호보드와 패스워드기호보드에 나열 표시하는 표시제어수단;

사용자가 패스워드 입력을 위해 실상매칭기호와 실상패스워드기호를 매칭시키기 위한 매칭수단;

매칭수단에 의해 매칭기호보드와 패스워드기호보드에 나열된 다수의 기호들이 매칭될 때 매칭된기호모임을 생성하여 인증처리수단으로 입력하는 매칭기호처리수단;

인증기준정보를 저장하는 메모리 및;

인증기준정보에 기초하여 입력된 매칭된기호모임에 포함된 실상매칭기호에 실상패스워드기호가 매칭되었는가를 판단하여 사용자의 메인 시스템으로의 접근을 허용 또는 거부하는 인증처리를 수행하는 인증처리수단을 포함하는 패스워드 시스템.

【청구항 2】

제1항에 있어서,

매칭기호보드 및 패스워드기호보드에 나열되는 기호들은 숫자, 문자, 도형, 그림 또는 이들의 조합을 포함하는 패스워드 시스템.

【청구항 3】

제2항에 있어서,

매칭기호보드 및 패스워드기호보드에 나열되는 기호들은 적어도 두 가지 이상의 서로 다른 색을 포함하여 표시되는 패스워드 시스템.

【청구항 4】

제1항에 있어서,

상기 기호발생수단은 매칭기호보드와 패스워드기호보드에 나열되는 기호들의 개수가 상호 동일하거나 또는 상호 동일하지 않은 것 중 어느 하나로 기호모임의 기호 개수를 결정하여 생성하는 패스워드 시스템.

【청구항 5】

제1항에 있어서,

표시제어수단은 매칭기호보드를 표시하지 않고 패스워드기호보드만 표시하고, 사용자는 매칭기호보드에 나열되는 기호들을 연상하고 연상된 실상매칭기호에 실상패스워드기호를 매칭시키는 패스워드 시스템.

【청구항 6】

제1항에 있어서,

적어도 한번 이상의 기호 매칭에 의해 다수의 실상매칭기호와 다수의 실상패스워드기호를 매칭시킬 때, 적어도 하나 이상의 매칭기호보드와 적어도 하나 이상의 패스워드기호보드가 동시에 표시되는 패스워드 시스템.

【청구항 7】

제1항에 있어서,

매칭기호보드 또는 패스워드기호보드에 나열된 기호들을 순환 이동시켜 실상매칭기호와 실상패스워드기호를 매칭시키는 패스워드 시스템.

【청구항 8】

제7항에 있어서,

매칭기호보드 또는 패스워드기호보드가 자동 순환하는 패스워드 시스템.

【청구항 9】

제1항 내지 제6항에 있어서,

실상매칭기호와 실상패스워드기호의 매칭을 위해 매칭기호보드 또는 패스워드기호보드의 순환 이동량을 직접 입력하는 패스워드 시스템.

【청구항 10】

제1항에 있어서,

매칭기호보드와 패스워드기호보드는 그래픽 사용자 인터페이스로 표시수단에 표시되는 패스워드 시스템.

【청구항 11】

제1항에 있어서,

표시수단은 매칭기호보드 또는 패스워드기호보드를 표시하고, 나열된 기호들을 순환 표시할 수 있는 기계적 메커니즘을 포함하는 패스워드 시스템.

【청구항 12】

제11항에 있어서,

기계적 메커니즘은 다수의 기호들을 순환 표시할 수 있는 다수개의 휠들과 다수개의 휠들을 제어하기 위한 휠 제어 버튼을 포함하는 패스워드 시스템.

【청구항 13】

제1항에 있어서,

기호발생수단은 매칭기호보드 및/또는 패스워드기호보드에 나열되는 기호들의 순서를 비복원으로 랜덤하게 생성하는 패스워드 시스템.

【청구항 14】

제1항에 있어서,

기호매칭에 의한 패스워드 입력과 함께 사용자 ID를 입력하는 패스워드 시스템.

【청구항 15】

제1항에 있어서,

기호발생수단은 인증기준정보에 기초하여 매칭기호보드 및/또는 패스워드기호보드에 표시될 기호모임을 생성하되, 사용자가 실상매칭기호와 실상패스워드기호를 매칭함에 있어서 소정의 범위 내에서 최소 순환이 이루지도록 기호들의 나열 순서를 결정하는 패스워드 시스템.

【청구항 16】

제1항에 있어서,

기호발생수단은 사용자 ID에 기초하여 인증기준정보를 패치하는 패스워드 시스템.

【청구항 17】

제1항에 있어서,

인증처리수단은 매칭된기호모임 또는 사용자 ID 중 어느 하나에 기초하여 인증기준정보를 패치하는 패스워드 시스템.

【청구항 18】

제1항에 있어서,

메모리에 저장된 인증기준정보는 실상매칭기호들의 모임과 실상패스워드기호들의 모임인 패스워드 시스템.

【청구항 19】

제18항에 있어서,

실상매칭기호모임과 실상패스워드기호모임에서 어느 하나가 다른 하나를 유도할 수 있을 때 유도할 수 있는 어느 하나만을 인증기준정보로 저장하는 투-패스워드인 패스워드 시스템.

【청구항 20】

제1항에 있어서,

메모리에 저장된 인증기준정보는 실상매칭기호들의 모임과 실상패스워드기호들의 모임을 각각 유도할 수 있는 정보인 패스워드 시스템.

【청구항 21】

제1항에 있어서,

통신망을 통해 메인 시스템에 접속하는 통신 단말기의 사용자 인터페이스에 표시 수단 및 매칭 수단이 구비되는 패스워드 시스템.

【청구항 22】

제21항에 있어서,

통신 단말기는 사용자의 패스워드 입력시 매칭기호보드 또는 패스워드기호보드의 순환 이동량을 메인 시스템으로 전송하되 전송 정보는 선택적으로 암호화되는 패스워드 시스템.

【청구항 23】

제21항에 있어서,

통신 단말기는 사용자 ID를 구비하고, 인증처리수단은 사용자 ID에 기초하여 인증기준정보를 패치하는 패스워드 시스템.

【청구항 24】

매칭에 기준이 되는 하나의 실상매칭기호와 이를 위장하기 위한 다수의 허상매칭기호를 포함하는 제1 기호모임, 실상매칭기호와 매칭되어야 하는 하나의 실상패스워드기호와 이를 위장하기 위한 다수의 허상패스워드기호를 포함하는 제2 기호모임을 생성하는 단계;

제 1 기호모임을 표시하기 위한 매칭기호보드와 제2 기호모임을 표시하기 위한 패스워드기호보드를 표시수단으로 표시하는 단계;

매칭기호보드의 실상매칭기호와 패스워드기호보드의 실상패스워드기호를 매칭수단에 의해 매칭시키는 것으로 투-패스워드를 입력하는 단계;

매칭기호보드와 패스워드기호보드의 기호들이 매칭되면 매칭된기호모임을 생성하여 인증처리수단으로 입력하는 단계 및;

인증처리를 위한 인증기준정보와 입력된 매칭된기호모임에 기초하여 사용자의 메인 시스템으로의 접급을 허락 또는 거부하는 인증처리 단계를 포함하는 패스워드 시스템의 사용자 인증 방법.

【청구항 25】

제24항에 있어서,

제 1 및 제2 기호모임을 생성하는 단계에서,

제1 기호모임과 제2 기호모임의 나열 순서를 어느 하나는 고정된 나열 순서를 갖고 다른 하나는 비복원 랜덤한 순서를 갖도록 하는 패스워드 시스템의 사용자 인증 방법.

【청구항 26】

제24항에 있어서,

제 1 및 제2 기호모임을 생성하는 단계에서,

제1 기호모임과 제2 기호모임의 나열 순서를 각각 비복원 랜덤한 순서를 갖도록 하는 패스워드 시스템의 사용자 인증 방법.

【청구항 27】

제25항 또는 제26항에 있어서,

제 1 및 제2 기호모임을 생성하는 단계는 인증기준정보를 패치하는 단계를 더 포함하고,

패치된 인증기준정보에 기초하여 제1 기호모임 및/또는 제2 기호모임을 생성하되 사용자가 실상매칭기호와 실상패스워드기호를 매칭 함에 있어서 소정 범위 이내의 순환이 이루어지도록 기호들의 나열 순서를 결정하는 패스워드 시스템의 사용자 인증 방법.

【청구항 28】

제24항에 있어서,

사용자 ID를 입력하는 단계를 더 포함하는 패스워드 시스템의 사용자 인증 방법.

【청구항 29】

제27항에 있어서,

제 1 및 제2 기호모임을 생성하는 단계는 입력된 사용자 ID에 기초하여 인증기준정보를 패치하는 단계를 더 포함하고,

패치된 인증기준정보에 기초하여 제1 기호모임 및/또는 제2 기호모임 생성하되 사용자가 실상매칭기호와 실상패스워드기호를 매칭함에 있어서 소정 범위 이내의 순환이 이루지도록 기호들의 나열 순서를 결정하는 패스워드 시스템의 사용자 인증 방법.

【청구항 30】

제24항에 있어서,

인증처리단계는

인증기준정보를 패치하는 단계;

인증기준정보로부터 실상매칭기호모임과 실상패스워드기호모임을 유도하는 단계;

유도된 실상매칭기호모임과 매칭되는 기호들을 매칭된기호모임에서 결정하는 단계;

결정된 기호모임과 유도된 실상패스워드기호모임을 비교하는 단계 및;

비교결과에 따라 사용자의 메인 시스템으로의 접근을 허락 또는 거부하는 단계를 포함하는 패스워드 시스템의 사용자 인증 방법.

【청구항 31】

제30항에 있어서,

사용자 ID를 입력하는 단계를 더 포함하고,

인증처리단계에서 입력된 사용자 ID에 기초하여 인증기준정보를 패치하는 패스워드 시스템의 사용자 인증방법.

【청구항 32】

제30항에 있어서,

인증처리단계에서 매칭된기호모임에 기초하여 인증기준정보를 패치하는 패스워드 시스템의 사용자 인증방법.

【청구항 33】

제30항에 있어서,

인증기준정보로부터 실상매칭기호모임과 실상패스워드기호모임을 유도하는 단계는,

인증기준정보가 '$X_1Y_1X_2Y_2X_3Y_3...X_{n-2}Y_{n-2}X_{n-1}Y_{n-1}X_nY_n$'일 때, 실상매칭기호를 '$X_1X_2X_3...X_{n-2}X_{n-1}X_n$'로 유도하고, 실상패스워드기호를 '$Y_1Y_2Y_3...Y_{n-2}Y_{n-1}Y_n$'로 각각 유도하는 패스워드 시스템의 사용자 인증방법.

【청구항 34】

제30항에 있어서,

인증기준정보로부터 실상매칭기호모임과 실상패스워드기호모임을 유도하는 단계는, 인증기준정보가 '$X_1X_2X_3...X_{n-2}X_{n-1}X_n$'일 때,

실상매칭기호를 '$X_1X_2X_3...X_{n-2}X_{n-1}$'로 유도하고, 실상패스워드기호를 '$X_2X_3...X_{n-2}X_{n-1}X_n$'로 각각 유도하는 패스워드 시스템의 사용자 인증방법.

【청구항 35】

제30항에 있어서,

인증기준정보로부터 실상매칭기호모임과 실상패스워드기호모임을 유도하는 단계는, 인증기준정보가 '$X_1X_2X_3...X_{n-2}X_{n-1}X_n$'일 때,

실상매칭기호를 '$X_1X_2X_3...X_{n-2}X_{n-1}X_n$'로 유도하고, 실상패스워드기호를 '$X_2X_3...X_{n-2}X_{n-1}X_nX_1$'로 각각 유도하는 패스워드 시스템의 사용자 인증방법.

【청구항 36】

제24항에 있어서,

매칭된기호모임 정보가 통신망을 통해 인증처리단계를 수행하는 인증처리수단으로 제공될 때, 매칭된기호모임 정보를 암호화하는 단계를 더 포함하는 패스워드 시스템의 사용자 인증 방법.

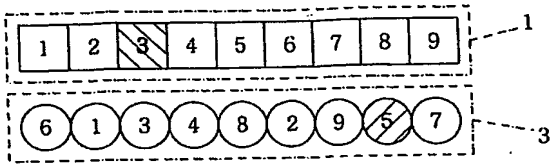
【청구항 37】

제24항에 있어서,

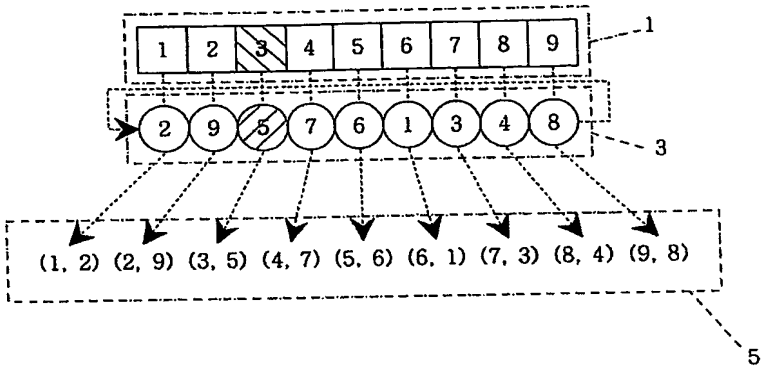
매칭된기호모임 정보가 통신망을 통해 인증처리단계를 수행하는 인증처리수단으로 제공될 때, 매칭된기호모임 정보를 통신 단말기를 표시하는 인덱스 정보로 사용하는 패스워드 시스템의 사용자 인증 방법.

【도면】

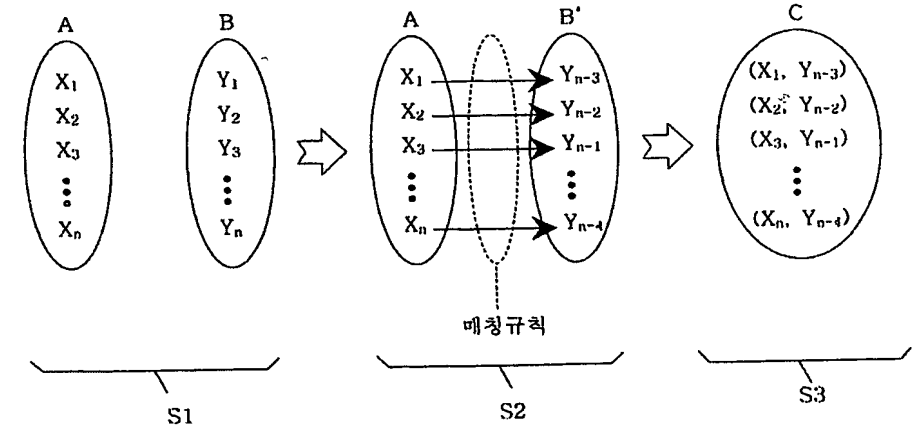
【도 1a】



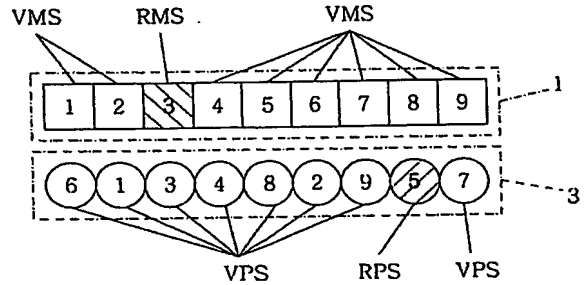
【도 1b】



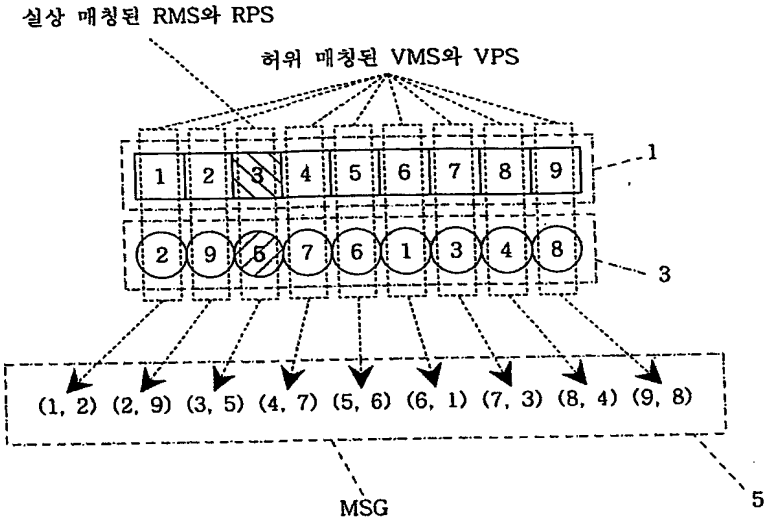
【도 2】



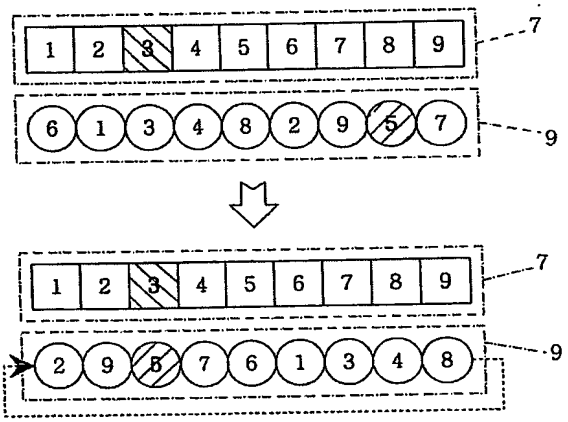
【도 3a】



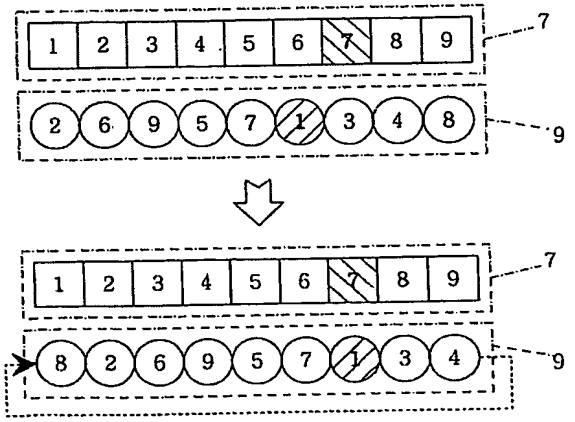
【도 3b】


실상 매칭된 RMS와 RPS
허위 매칭된 VMS와 VPS
1 2 3 4 5 6 7 8 9
2 9 5 7 6 1 3 4 8
1
3
(1, 2) (2, 9) (3, 5) (4, 7) (5, 6) (6, 1) (7, 3) (8, 4) (9, 8)
MSG
5

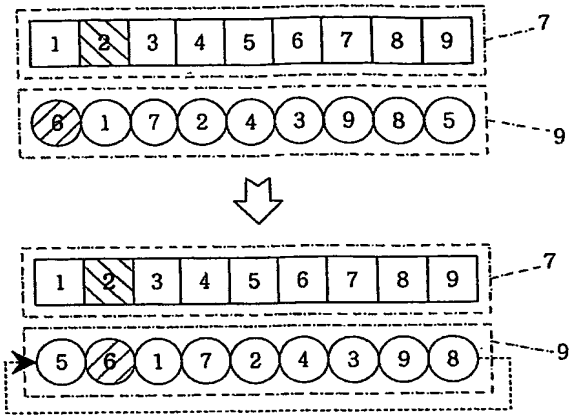
【도 4a】


1 2 3 4 5 6 7 8 9
6 1 3 4 8 2 9 5 7
7
9
1 2 3 4 5 6 7 8 9
2 9 5 7 6 1 3 4 8
7
9

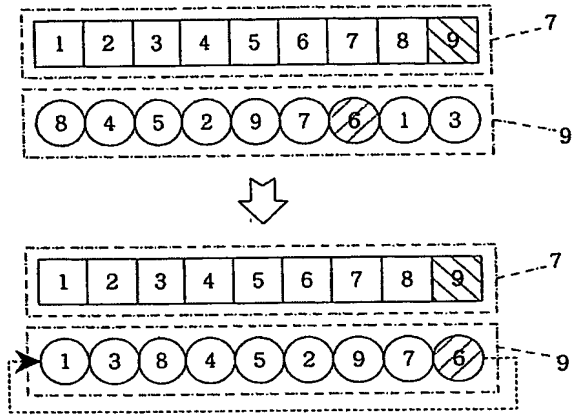
【도 4b】


1 2 3 4 5 6 7 8 9
2 6 9 5 7 1 3 4 8
7
9
1 2 3 4 5 6 7 8 9
8 2 6 9 5 7 1 3 4
7
9

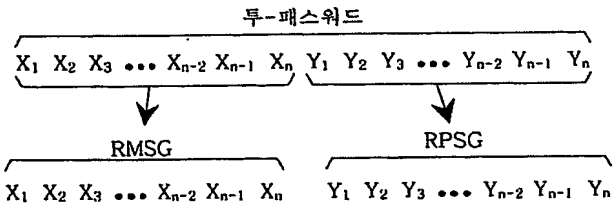
【도 4c】



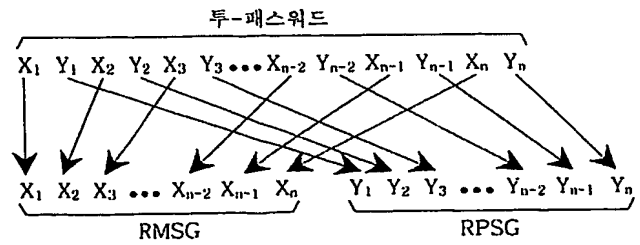
【도 4d】



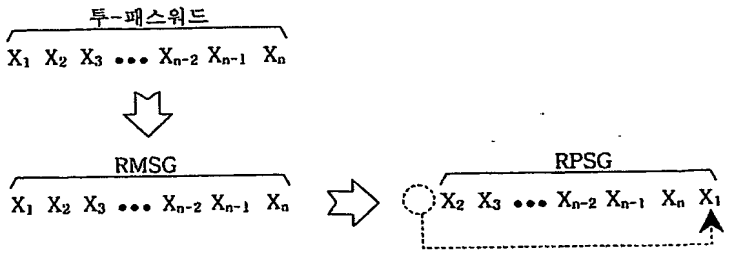
【도 5a】



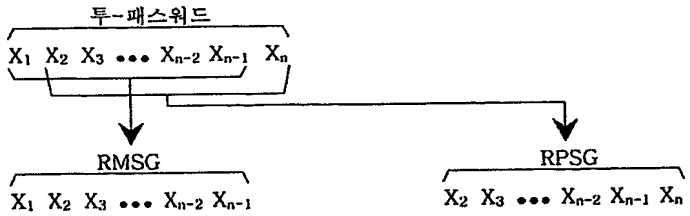
【도 5b】



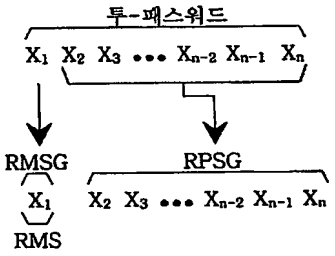
【도 5c】



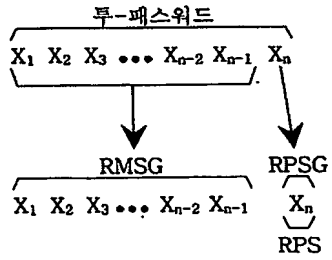
【도 5d】



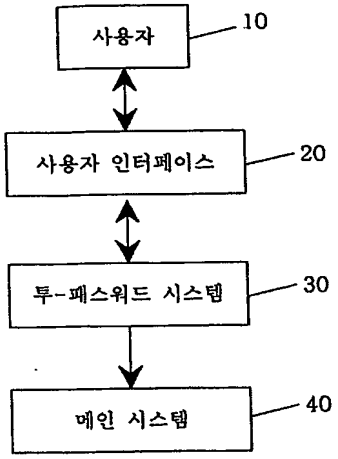
【도 6a】



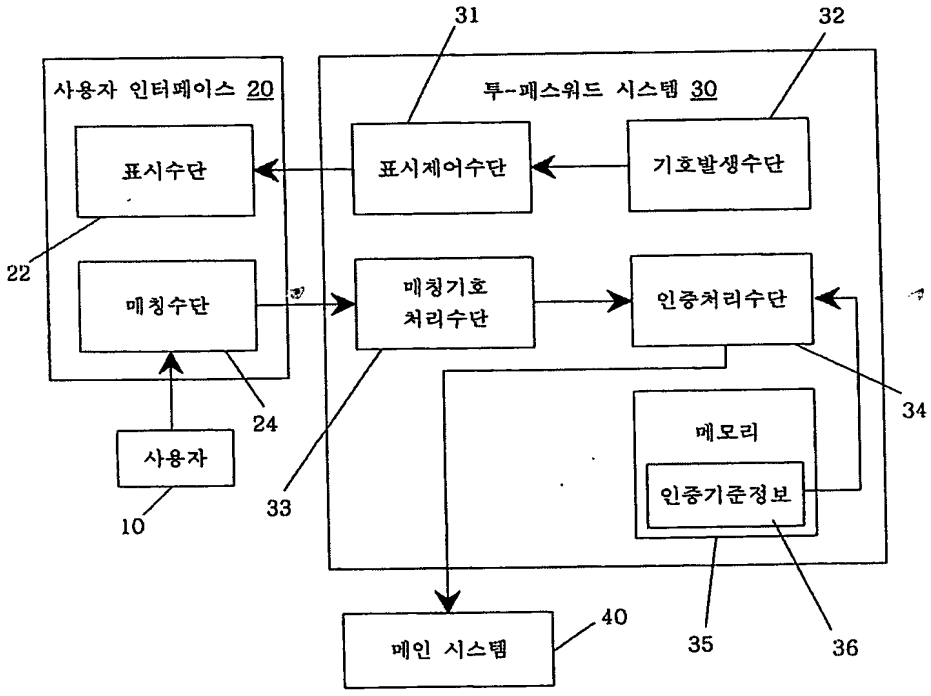
【도 6b】



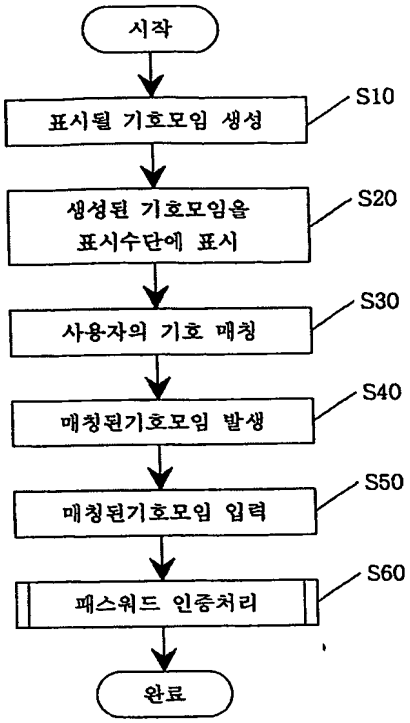
【도 7】


사용자
10
사용자 인터페이스
20
투-패스워드 시스템
30
메인 시스템
40

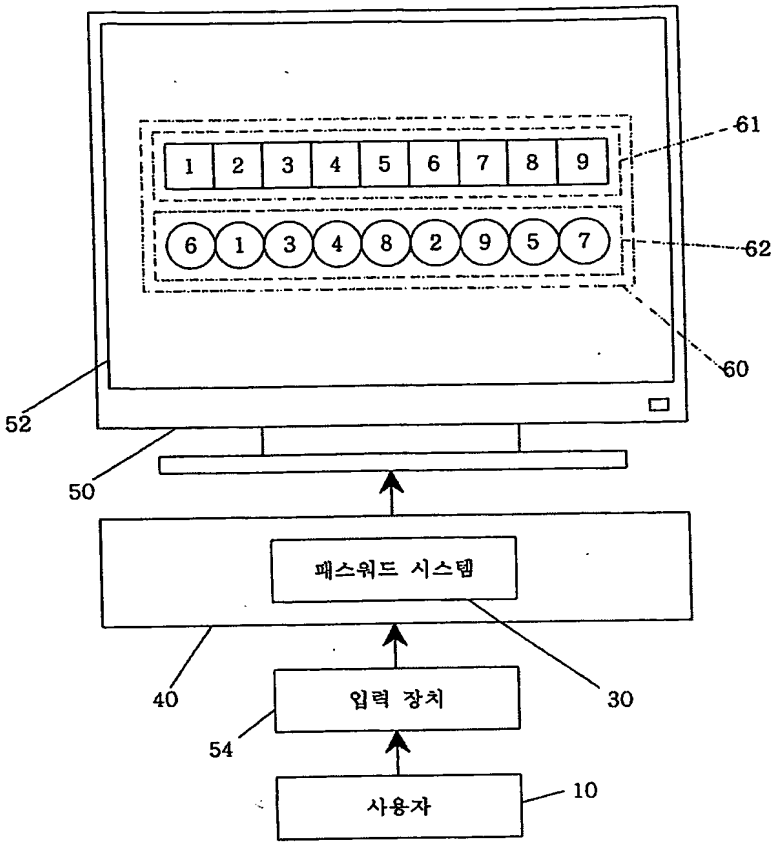
【도 8】


31
32
사용자 인터페이스 20
투-패스워드 시스템 30
표시수단
표시제어수단
기호발생수단
22
매칭수단
매칭기호 처리수단
인증처리수단
34
메모리
인증기준정보
24
사용자
10
33
35
36
메인 시스템
40

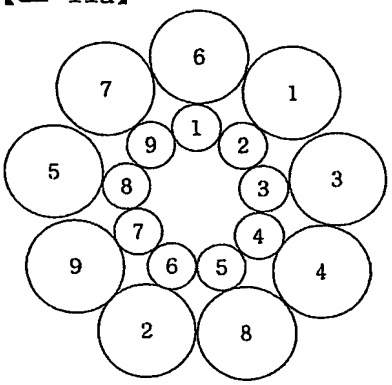
【도 9】


시작
표시될 기호모임 생성
S10
생성된 기호모임을 표시수단에 표시
S20
사용자의 기호 매칭
S30
매칭된기호모임 발생
S40
매칭된기호모임 입력
S50
패스워드 인증처리
S60
완료

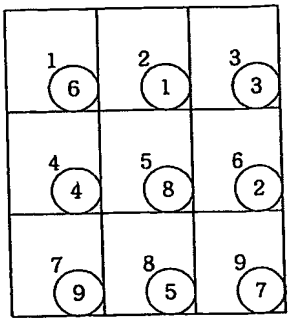
【도 10】


1 2 3 4 5 6 7 8 9
6 1 3 4 8 2 9 5 7
61
62
60
52
50
패스워드 시스템
40
30
입력 장치
54
사용자
10

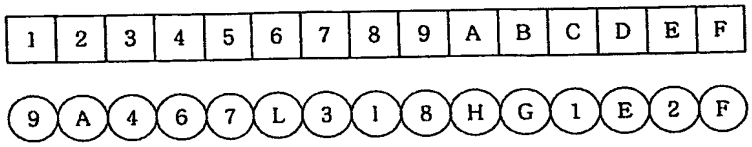
【도 11a】


6
7
1
1
9
2
5
8
3
3
7
4
9
6
5
4
2
8

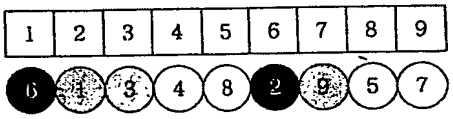
【도 11b】



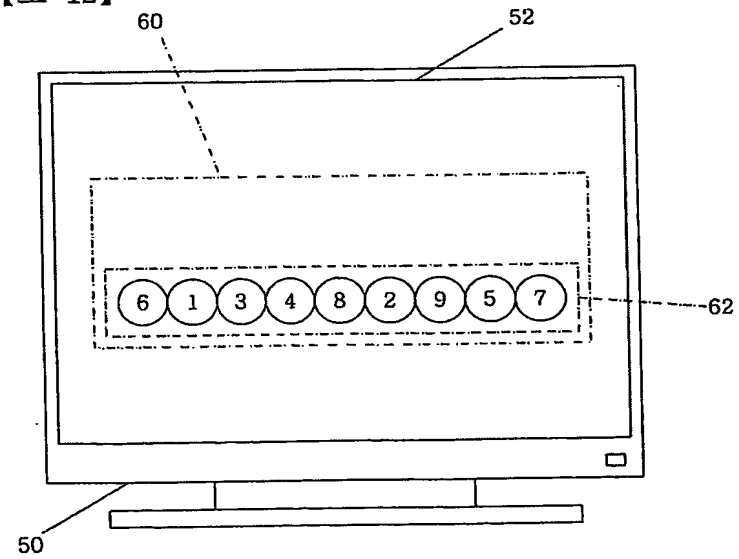
【도 11c】



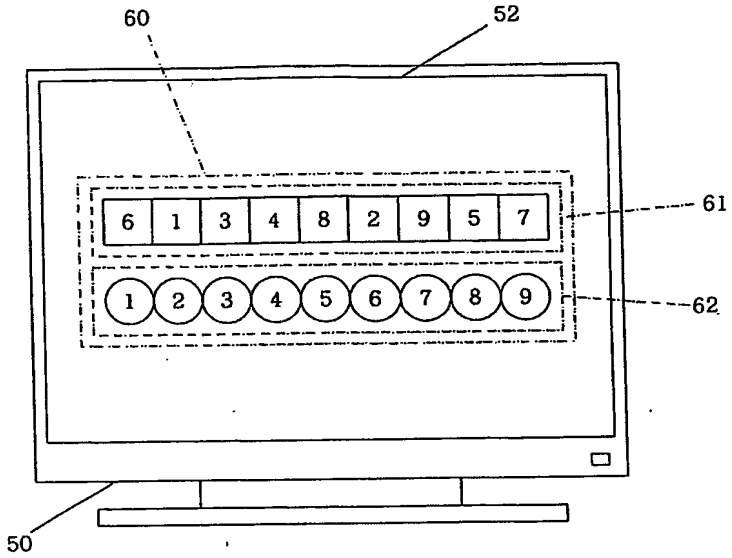
【도 11d】



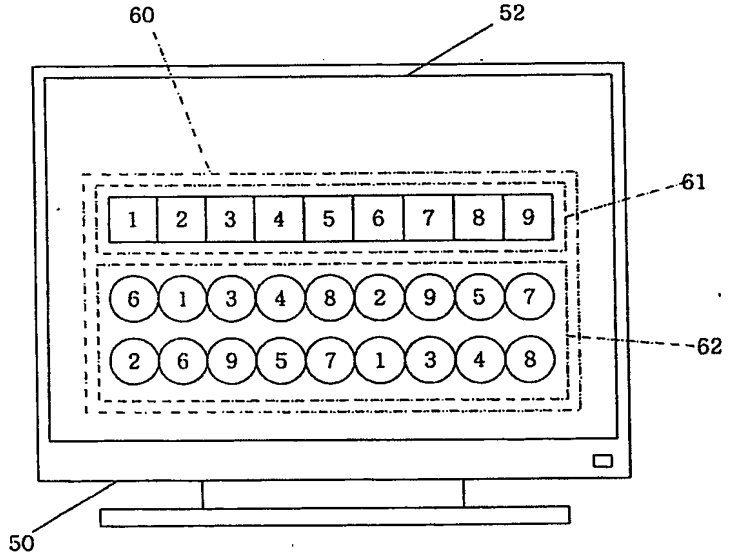
【도 12】



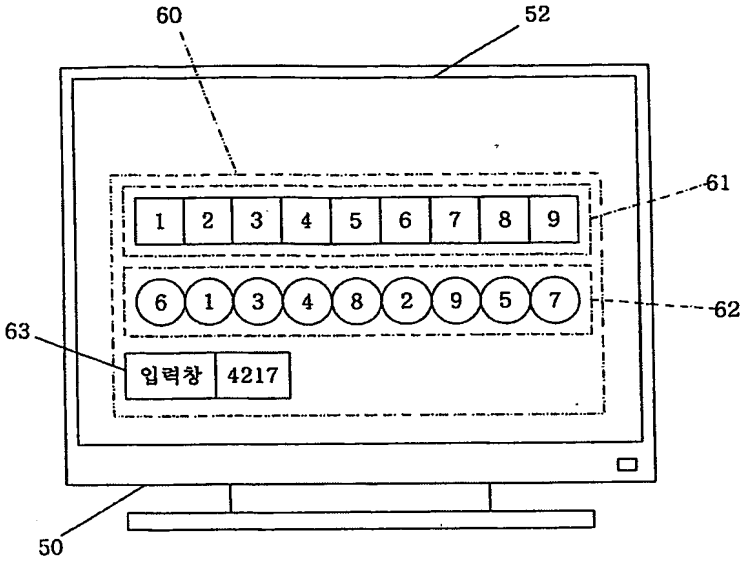
【도 13】


60
52
6 1 3 4 8 2 9 5 7
61
1 2 3 4 5 6 7 8 9
62
50

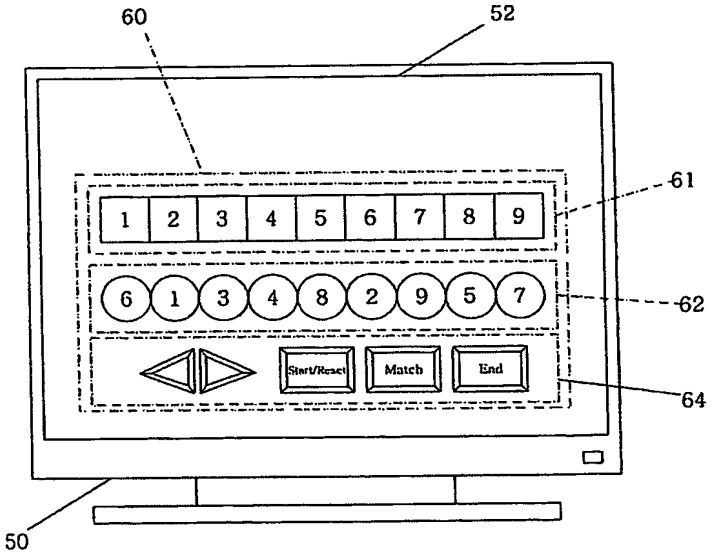
【도 14】


60
52
1 2 3 4 5 6 7 8 9
61
6 1 3 4 8 2 9 5 7
2 6 9 5 7 1 3 4 8
62
50

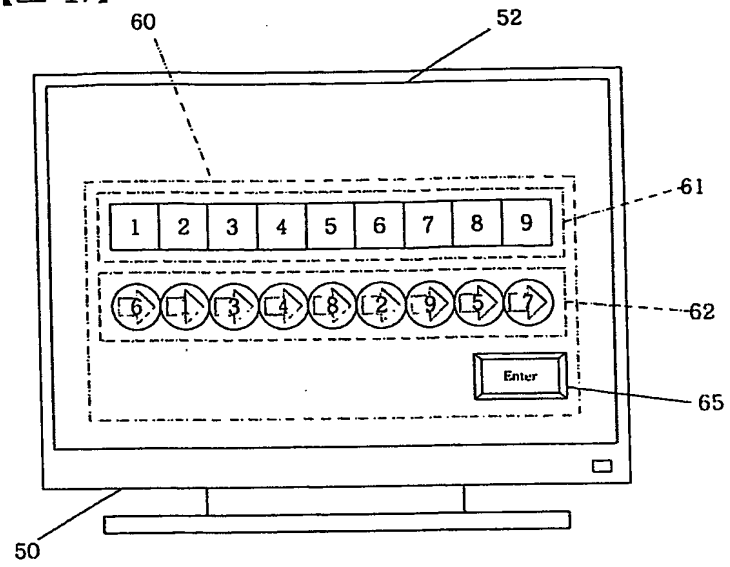
【도 15】


60
52
61
1 2 3 4 5 6 7 8 9
6 1 3 4 8 2 9 5 7
62
63
입력창 4217
50

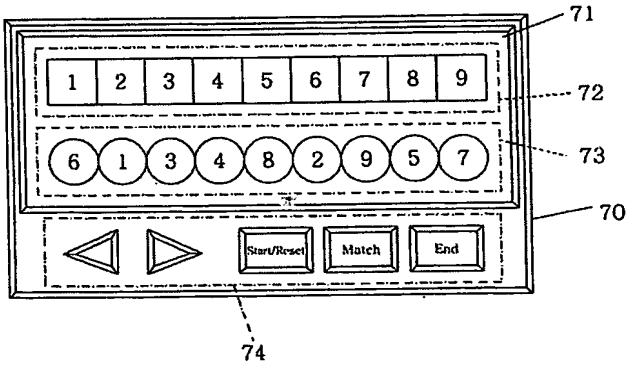
【도 16】


60
52
61
1 2 3 4 5 6 7 8 9
6 1 3 4 8 2 9 5 7
62
Start/Reset
Match
End
64
50

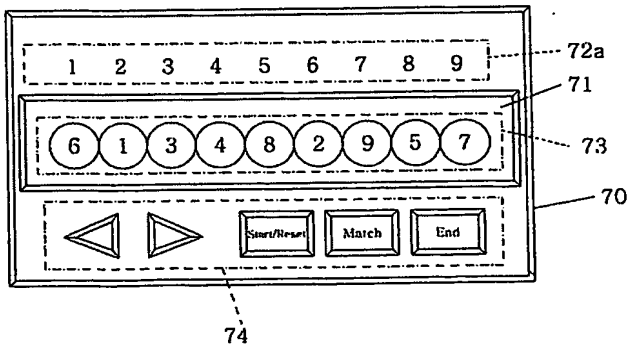
【도 17】


60
52
61
1 2 3 4 5 6 7 8 9
6 1 3 4 8 2 9 5 7
62
Enter
65
50

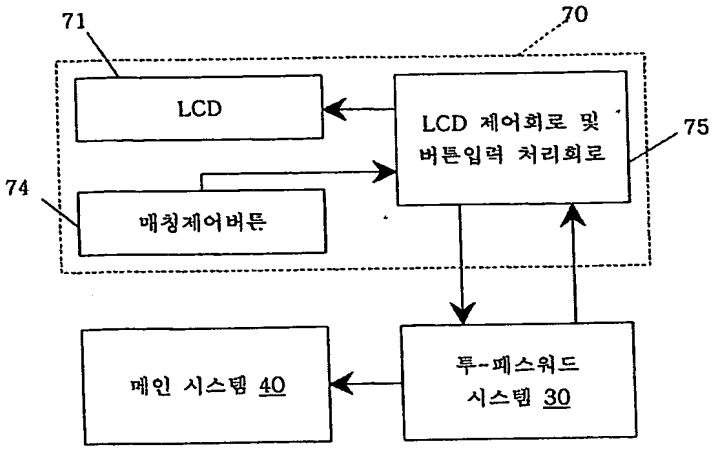
【도 18】


71
1 2 3 4 5 6 7 8 9
72
6 1 3 4 8 2 9 5 7
73
70
Start/Reset
Match
End
74

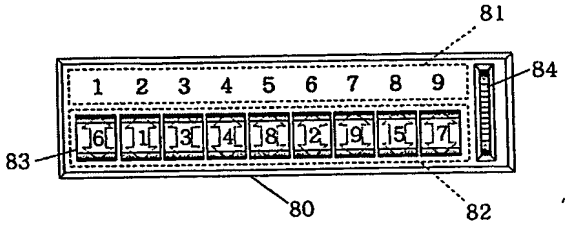
【도 19】


1 2 3 4 5 6 7 8 9
72a
71
6 1 3 4 8 2 9 5 7
73
70
Start/Reset
Match
End
74

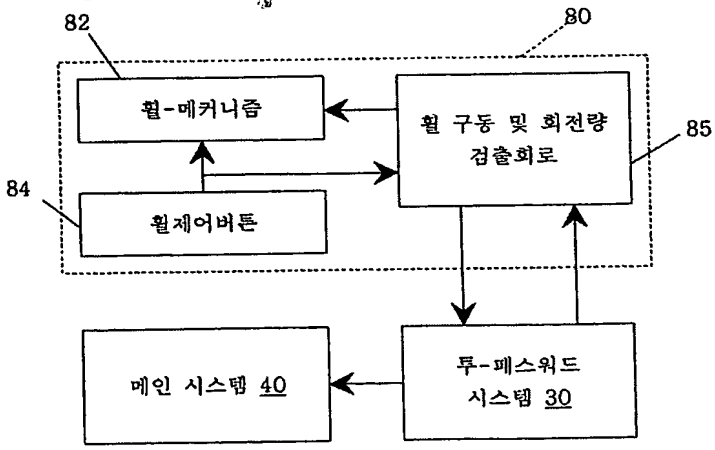
【도 20】


71
70
LCD
LCD 제어회로 및
버튼입력 처리회로
75
74
매칭제어버튼
메인 시스템 40
투-페스워드
시스템 30

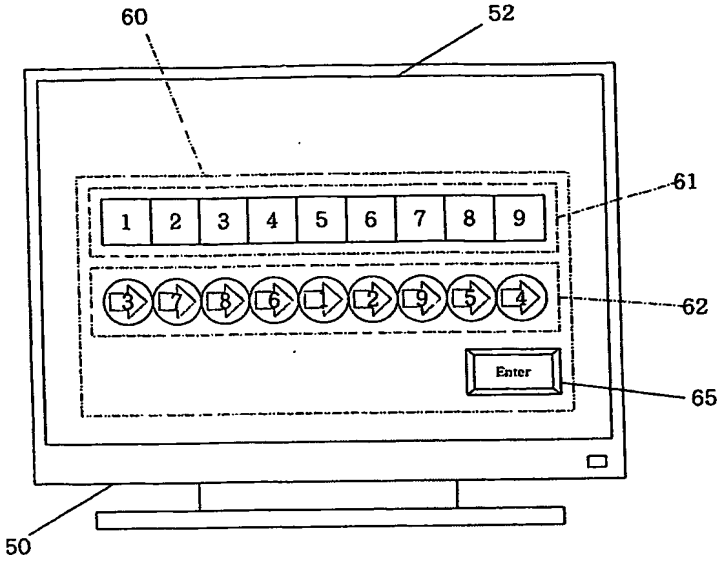
【도 21】


81
1 2 3 4 5 6 7 8 9
84
83
80
82

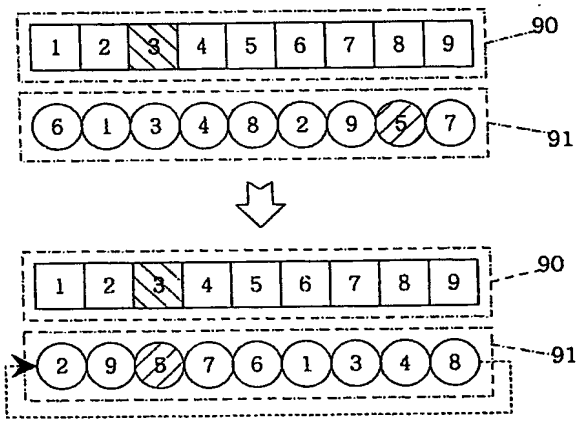
【도 22】


82
80
휠-메커니즘
휠 구동 및 회전량
검출회로
85
84
휠제어버튼
메인 시스템 40
투-페스워드
시스템 30

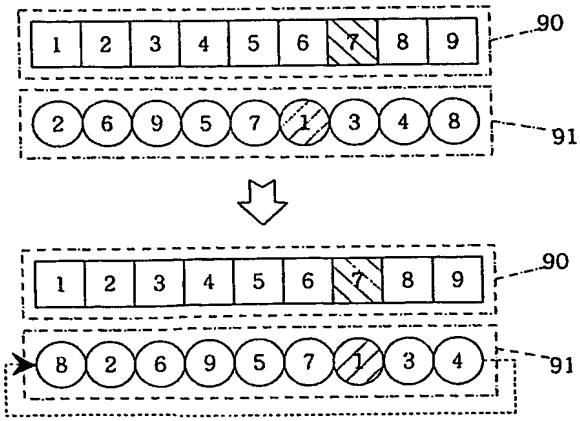
【도 23】



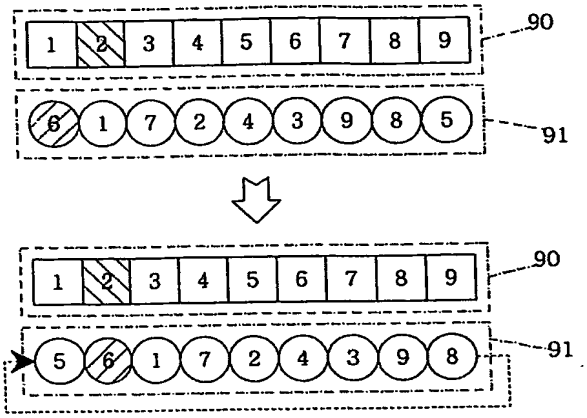
【도 24a】



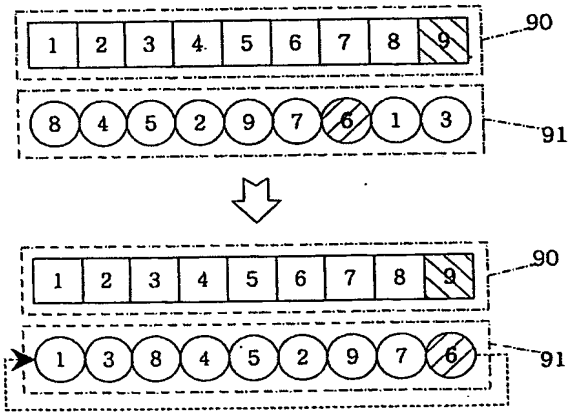
【도 24b】



【도 24c】



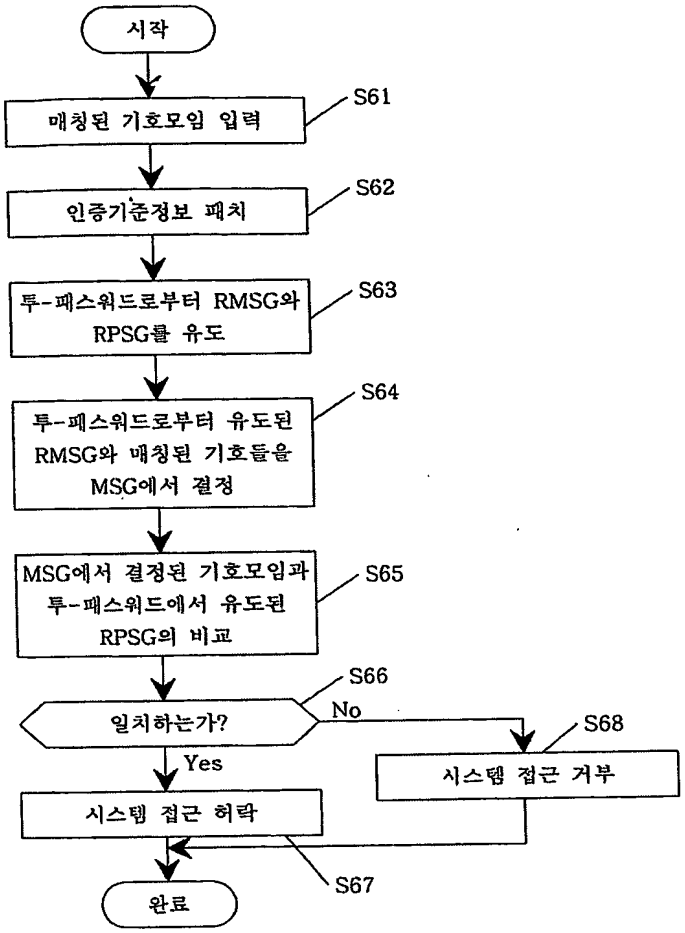
【도 24d】



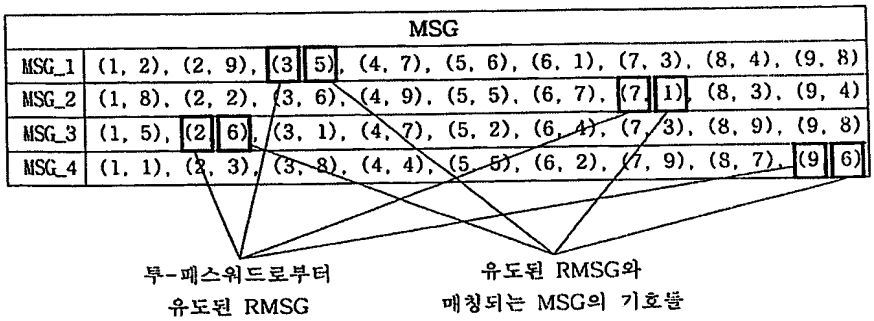
【도 25】

	MSG
MSG_1	(1, 2), (2, 9), (3, 5), (4, 7), (5, 6), (6, 1), (7, 3), (8, 4), (9, 8)
MSG_2	(1, 8), (2, 2), (3, 6), (4, 9), (5, 5), (6, 7), (7, 1), (8, 3), (9, 4)
MSG_3	(1, 5), (2, 6), (3, 1), (4, 7), (5, 2), (6, 4), (7, 3), (8, 9), (9, 8)
MSG_4	(1, 1), (2, 3), (3, 8), (4, 4), (5, 5), (6, 2), (7, 9), (8, 7), (9, 6)

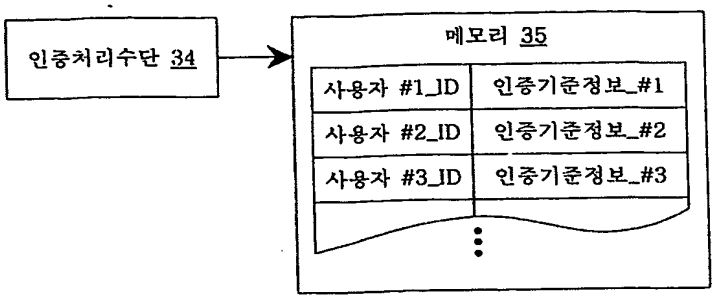
【도 26】


시작
매칭된 기호모임 입력
S61
인증기준정보 패치
S62
투-패스워드로부터 RMSG와 RPSG를 유도
S63
투-패스워드로부터 유도된 RMSG와 매칭된 기호들을 MSG에서 결정
S64
MSG에서 결정된 기호모임과 투-패스워드에서 유도된 RPSG의 비교
S65
일치하는가?
S66
No
S68
시스템 접근 거부
Yes
시스템 접근 허락
S67
완료

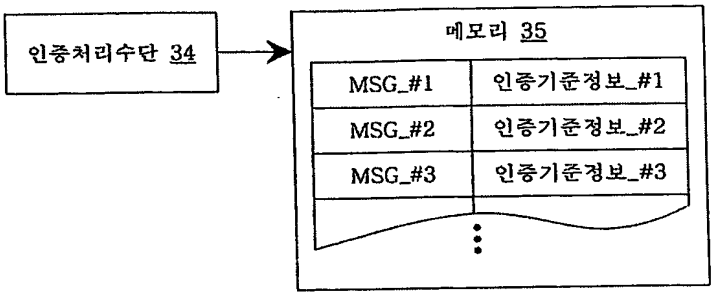
【도 27】


MSG
MSG_1 (1, 2), (2, 9), (3, 5), (4, 7), (5, 6), (6, 1), (7, 3), (8, 4), (9, 8)
MSG_2 (1, 8), (2, 2), (3, 6), (4, 9), (5, 5), (6, 7), (7, 1), (8, 3), (9, 4)
MSG_3 (1, 5), (2, 6), (3, 1), (4, 7), (5, 2), (6, 4), (7, 3), (8, 9), (9, 8)
MSG_4 (1, 1), (2, 3), (3, 8), (4, 4), (5, 5), (6, 2), (7, 9), (8, 7), (9, 6)
투-패스워드로부터 유도된 RMSG
유도된 RMSG와 매칭되는 MSG의 기호들

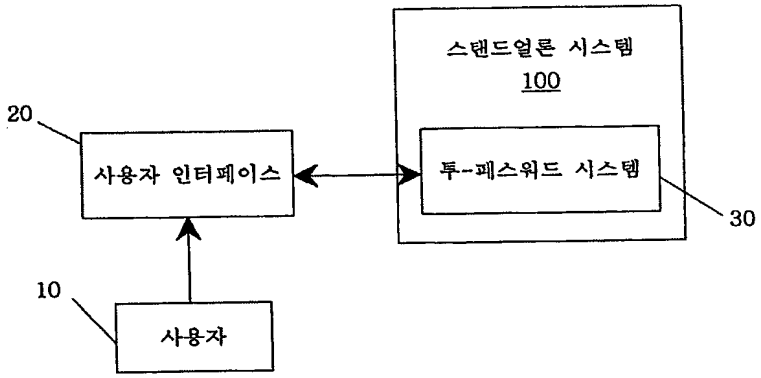
【도 28】


인증처리수단 34
메모리 35
사용자 #1_ID
인증기준정보_#1
사용자 #2_ID
인증기준정보_#2
사용자 #3_ID
인증기준정보_#3

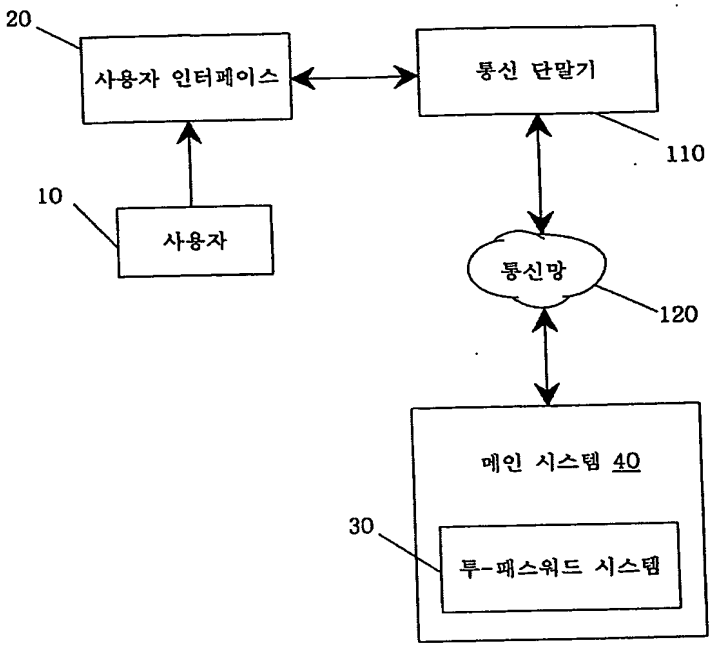
【도 29】


인증처리수단 34
메모리 35
MSG_#1
인증기준정보_#1
MSG_#2
인증기준정보_#2
MSG_#3
인증기준정보_#3

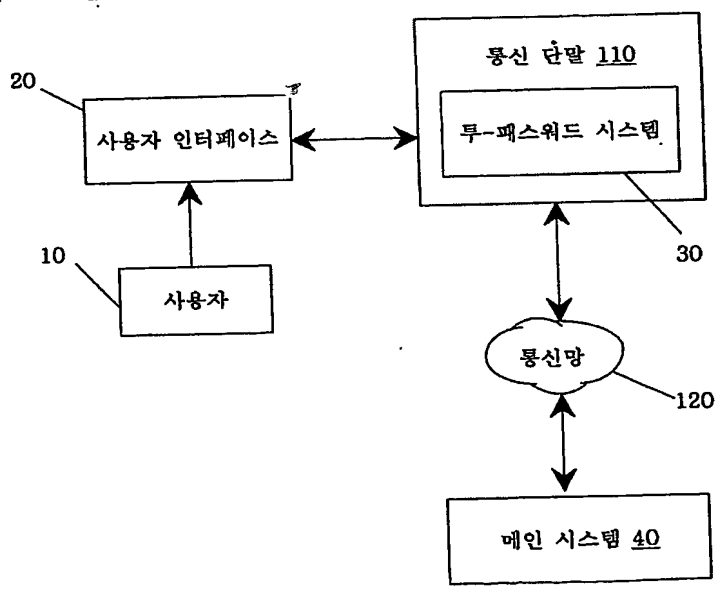
【도 30】


스탠드얼론 시스템
100
20
사용자 인터페이스
투-패스워드 시스템
30
10
사용자

【도 31】


20
사용자 인터페이스
통신 단말기
110
10
사용자
통신망
120
메인 시스템 40
30
투-패스워드 시스템

【도 32】


통신 단말 110
20
사용자 인터페이스
투-패스워드 시스템
30
10
사용자
통신망
120
메인 시스템 40